Voortschrijdend jaarplan CIP. Datum 1-12-2016

Planperiode: 1-1-2017 – 31-12-2017

Inhoudsopgave

1. Over CIP.

1.1. Wat is CIP?

CIP staat voor 'Centrum Informatiebeveiliging en Privacybescherming'. Het is een samenwerkingsverband van deelnemende overheidsorganisaties (de participanten) en een aantal marktpartijen (de kennispartners), die willen bijdragen aan het ontwikkelen, delen en ontsluiten van kennis en 'good practices' op het gebied van Informatieveiligheid en Privacy. Het netwerk staat open voor medewerkers uit alle lagen van de overheid. De kennispartners zijn marktpartijen die met gesloten beurs deelnemen in het kennisnetwerk en dat in een convenant bekrachtigen.

1.2. Doelstelling

Door kennisdeling en krachtenbundeling bijdragen aan het tot stand brengen van een aanzienlijk hoger niveau van beveiliging, van zowel de overheidsorganisaties afzonderlijk als de ketens die zij onderling vormen.

1.3. Werkwijze

Het CIP werkt op basis van het principe "vóór allen, dóór allen": samen vormen we het CIP. De aangesloten organisaties werken daarin mee met een zelf te bepalen aantal uren en inzet. Een klein kernteam organiseert de samenwerking.

1.4. Wat heeft u aan CIP

Door het jaar heen worden tal van kennissessies georganiseerd in Domeingroepen en zg. 'Practitioners Communities'. Vanuit deze subcommunities is een scale van nuttige, vrij bruikbare producten ontwikkeld. Het betreft kaders voor ontwikkeling van veilige software en mobiele apps (Grip op Secure Software, SSD), handreikingen voor verantwoord gegevensgebruik (Grip op Privacy), Materiaal voor gebruik in bewustwordingsprogramma's (Filmmateriaal , e-Learning-modules) en nog veel meer.

Alles is te vinden op de site www.cip-overheid.nl.

Daarnaast kunnen overheidsmensen en kennispartners aansluiten op de besloten samenwerkingsomgeving cip.pleio.nl, waar u nog veel meer materiaal kunt vinden en verdere kennis kunt opdoen door aan te sluiten bij - en deel te nemen aan - discussies, de 'Privacy-vraagbaak' etc.

1.5. Over de jaarplancyclus

CIP werkt met een 4-kwartaals voortschrijdend jaarplan dat elk kwartaal wordt geijkt. Het jaarplan CIP bestaat uit een globale vooruitblik die kan worden gezien als managementsamenvatting (Hoofdstuk 2) en een overzicht van agendapunten die de leidraad vormen voor het handelen in de planperiode. Deze agendapunten zijn verdeeld in een algemeen deel en een deel per aandachtsgebied. Ze zijn opgenomen in hoofdstuk 3 van dit document.

Bijlagen bij dit plan zijn:

- Releaseplanning. Een overzicht van geplande nieuwe releases van CIP-producten. Eveneens vier kwartalen voortschrijdend. Bij iedere kwartaalijking wordt ook een kwartaal toegevoegd aan het releaseplan.
- Activiteitenplanning. Een planning van bijeenkomsten en CIP-activiteiten. Deze wordt wekelijks actueel gehouden en dient eveneens als bijlage voor het jaarplan. Ook hier wordt een tijdvenster gehanteerd van vier kwartalen voortschrijdend.
- Productenoverzicht. Dit is het overzicht van beschikbare producten van het CIP.

2. Vooruitblik planperiode / Managementsamenvatting

De ontwikkeling van CIP begon met kennisdeling in sessies, werd uitgebreid met het ontwikkelen van kennisproducten en vervolgens met implementatie-ondersteunende activiteiten als practitionerscommunities en tot slot (in 2016) met de start van 'netwerk-gebaseerde' dienstverlening.

Door aan te sluiten op enerzijds de vraag naar specifieke kennis en - daarmee samenhangend - ook de energie die in het netwerk aanwezig is, konden we steeds relevant blijven voor het netwerk, dat een gestage groei heeft doorgemaakt.

Ook de komende periode blijft het van groot belang de aansluiting te blijven vinden bij energie en interesse. Alleen dan zal het mogelijk blijven ook capaciteit uit het netwerk te blijven betrekken op de ontwikkeling en actualisering van de kennisproducten.

Op hoofdlijnen voorzien we de volgende ontwikkelingen in de planperiode.

2.1. Kennisdeling.

Naast de voorjaars- en najaarsconferentie zetten we de bijeenkomsten voort van domeingroepen en practitioners communities door het jaar heen voor uiteenlopende thema's. Hierbij voorzien we een toename van uitwisseling via cip.pleio, gepaard aan een kleine vermindering van het aantal bijeenkomsten.

Kennisdeling en communicatie over de activiteiten en producten krijgt een nog grotere aandacht en wordt in dep planperiode breder ondersteund met digitale hulpmiddelen. Zo heeft CIP een partnerpagina bij iBestuur en zal de NORA-Wiki worden gebruikt voor het ontsluiten van de CIP-uitwerkingen van de BIR/BIO. We verwachten veel accent bij het thema Privacy. Men name de meldplicht en de consequenties van de Europese wetgeving houden de participanten bezig. Daarnaast blijft Secure software development actueel, waarbij het blijven stimuleren van de toename van het gebruik voorop staat.

De toename van de populatie (730 op het moment van schrijven) op cip.pleio schept nieuwe mogelijkheden voor digitale uitwisseling binnen het netwerk.

Ook de vakpers zal regelmatig worden gevoed met artikelen en verwijzingen naar CIP-materiaal.

In de planperiode zal ook aandacht worden besteed aan agendering op de bestuurstafel van de thema's informatieveiligheid en privacy. We trekken hierin samen op met iBestuur. In januari plannen we een combinatie van een mini-conferentie, met bestuurstafel en een uitgave over Privacy.

2.2. Productontwikkeling

Aangezien de hoeveelheid beschikbare CIP-producten groot is geworden, groeit de relatieve inspanning aan onderhoud. De ontwikkeling van geheel nieuwe producten zal dan ook iets afnemen. Daartoe zal worden gewerkt met een releasekalender om het onderhoud meer planmatig te kunnen vormgeven.

De privacy-producten zullen moeten worden geactualiseerd met de gevolgen van de Europese wetgeving op het moment dat dit mogelijk is. CIP zal daartoe betrokken blijven bij de nadere uitwerking binnen de Nederlandse wetgeving van de AVG en zal ook de gevolgen van de wetgeving verwerken in de Privacy Baseline en de handreikingen Privacy by Design en Privacy governance. Voor management zal een Handreiking worden opgeleverd voor Privacy management.

Ontwikkeling van de BIO en de thematische-uitwerkingen/handreikingen zal verder ter hand worden genomen. Enerzijds wordt hiermee gewerkt aan de eenheid binnen de overheid, anderzijds komen we met de handreiking te hulp bij de concrete implementatie in organisaties.

T.b. de ontwikkeling van veiligheidsbewustzijn blijven we werken aan de uitbreiding van CIP-cast productlijn en ook aan de ontwikkeling van serious gaming. E-learning krijgt geen aandacht in de planperiode. De eerder ontwikkelde modules blijven wel beschikbaar.

2.3. Implementatie en dienstverlening

Het gebruik van CIP-producten in het netwerk neemt toe. Verder stimulering daarvan heeft hoge prioriteit in de CIP-agenda. Uiteindelijk is de doelstelling van vergroting van de informatieveiligheid van de overheidsdienstverlening juist daarbij gebaat.

Binnen practitioners communities wordt het gebruik gestimuleerd door het delen van praktijkervaringen met de producten. Tevens worden de ervaringen gebruikt als input voor actualisering van de producten.

Ook de netwerk-gebaseerde dienstverlening zal veel aandacht krijgen toenemen. We verwachten (en sturen op) een sterke voortzetting van de uitvoering van de serious games van CIP, waarmee wordt bijgedragen aan zowel veiligheidsbewustzijn als vaardigheden i.k.v. crisismanagement. Daarnaast voorzien we een sterke ontwikkeling van de Privacy Vraagbaak. Voor de dienst 'Peer Review' sturen we aan op een rustige verdere ontwikkeling. Rond verschillende onderwerpen (In ieder geval privacy en SSD) zijn er workshops die aangeboden worden i.s.m. kennispartners als PBLQ.

2.4. Interbestuurlijke relaties

CIP werk interbestuurlijk samen met meerdere instanties en platforms binnen de overheid. Dit blijft van belang met het oog op afstemming (wie doet wat), de verankering van de CIP-producten en –bijeenkomsten als ook de brede ontsluiting van kennis. Regelmatige uitwisseling wordt voortgezet met de volgende instanties.

- Informatiebeveiligingsdienst Gemeenten (IBD). Met IBD vindt regelmatig kennisuitwisseling plaats. Dir-CIP is ook lid van de Adviesraad IBD.
- De stichting in oprichting voor normering van opleidingen en kwalificatie van de beroepsgroep. Dir-CIP neemt ook deel aan het bestuur
- Subcommissie IB van het CIO-platform. CIP is lid.
- Kennisnetwerk van het NCSC.
- Ministerie van BZK, zowel met de organisatie van CIO-rijk als het onderdeel DIO. Specifiek speelt het overnemen door CIP van delen van de producten en netwerk van iBewustzijn.
- Ministerie van EZ en ECP. Op het gebied van Privacy en Secure Software wordt samengewerkt.
- Interbestuurlijke Werkgroep Normatiek, waarin de bijdrage centraal staat aan de ontwikkeling naar de BIO en de thema-uitwerkingen daarbinnen (concrete handreikingen voor implementatie).
- Lidmaatschap van de SZW-Werkgroep die de lokale wetgeving voorbereidt binnen de Algemene Verordening Gegevensbescherming.
- iBestuur. CIP is als kennispartner betrokken bij de redactie van iBestuur congres en specials. CIP heeft ook een partnerpagina op de site van iBestuur.

3. Agendapunten in de planperiode

3.1. Algemeen

Voor CIP als geheel gelden de volgende agendapunten.

- Meer aandacht zal uitgaan naar het beheer van de producten. Het is van belang om producten aangepast te houden aan de actualiteit en van tijd tot tijd geactualiseerde versies aan te bieden in het netwerk.
- Verder tot bloei brengen van de diensten. Deze diensten zijn: Collegiale Toetsingen, Privacy-vraagbaak, workshops privacy, uitvoering van de 'Serious Game Crisis' en de gemeentevariant van deze game. Later in de planperiode volgt ook de nu in ontwikkeling zijnde Ketengame.
- Bij de diensten gaan we nog sterker accent leggen op het benutten van de verbreidingsstrategie die we hanteren voor de Crisisgame. Dit moet leiden tot veelvuldig uitvoering van de diensten doordat leden uit het netwerk hierbij ingeschakeld worden.
- Meer aandacht voor het bedienen van het bestuurlijke niveau. Doordat CIP zich vooral toegelegd heeft op kennisdeling en het vakgebied toch redelijk specialistisch is, ligt de PDC vooral op tactisch en operationeel vlak. Het is van belang meer werk te maken van het betrekken van bestuurders bij de IB&P-problematiek. We willen een rondetafelconcept ontwikkelen dat herhaalbaar is voor verschillende groepen bestuurders en hoger management en daarmee in de planperiode een start maken.
- De ontwikkeling van de Baseline Informatiebeveiliging Overheid: het samenbrengen van de verschillende baselines tot één baseline. CIP draagt hieraan bij binnen de interbestuurlijke 'Werkgoep Normen'. Accenten voor het CIP-netwerk liggen op de thematische uitwerkingen met SIVA, die nuttige handvatten opleveren voor de concrete implementatie van maatregelen.
- De opbouw van ISOR (Information Security Object Repository), waarin worden ondergebracht alle door CIP beschreven maatregelen binnen de thematische uitwerkingen (zoals SSD, Privacy Baseline, etc). ISOR wordt ondergebracht in NORA en maakt gebruik van de NORA-Wiki, waardoor het bereik in de overheid maximaal wordt.
- Communicatie en het bevorderen van de bekendheid en het gebruik van CIP-producten blijft een belangrijk speerpunt. Hiermee bevorderen we de Veiligheidsbewustzijn alsook de feitelijke implementatie van het gedachtegoed en de producten. Enkele digitale kanalen die we zullen benutten zijn: NORA en de website iBestuur, waar CIP een partnerpagina krijgt. Daarnaast blijven we onze eigen sites alsook de vakpers benutten voor communicatie. Ook de verbindingen die CIP heeft met CIO-platform (Subcommissie Informatiebeveiliging), VNG (onder meer de Adviesraad Informatiebeveiligingsdienst), Forum Standaardisatie, iBewustzijn Rijk, ECP en meer, blijven van belang voor wederzijdse uitwisseling en verspreiding van kennis.
- Blijvende aandacht voor persoonlijke communicatie brengt in nog steeds groeiende netwerk een toenemende beheerlast met zich mee van het 'CRM' (zijnde de optelsom tussen de netwerkregistratie en de pleio-registratie).
- Vitaal houden van de verschillende communities door nieuwe vormen en werkwijzen aan te bieden en aan te sluiten bij thema's die actueel zijn. Door de grote toename van deelname op cip.pleio, kan een deel van de communicatie in bijeenkomsten verschuiven naar digitale communicatie.

3.2. Domein Awareness

Voor Domeingroep Awareness is de invulling als volgt.

- Cip-casts. Vervolgen/uitbreiden van de reeks CIP casts met nieuwe onderwerpen en verdiepingen. Hierbij wordt ook aandacht gegeven aan het werven van nieuwe sponsoren.
- Serious Game Crisis. Continueren/aanbieden van sessies.
- Awareness in relatie tot Integrale veiligheid en de Bestuurstafel. Aanzet geven voor bestuurstafel.
- Praco Awareness met alle betrokken partijen continueren. Meerdere keren plannen van bijeenkomsten met aansprekende thema's.
- Collegiale intervisie promoten (op basis van behoeftepeiling) tussen CIP-deelnemers vanaf najaar 2016.
- Nauwere samenwerking zoeken met RijksBVA en Integraal Veilig Hoger Onderwijs, fase 3 (en mogelijk volgend jaar fase 4). Loopt vanaf najaar 2016.
- Penetratietesten (laten) uitvoeren, fysieke beveiliging, ethische hackers – behoeftepeiling in gang zetten in najaar 2016.
- Format ontwikkelen om bij grotere incidenten direct adequaat te kunnen adviseren (kan direct worden getest wanneer zich groter incident voordoet).
- Onderwerpen en goede sprekers verzamelen voor lunchlezingen op locatie van CIP-deelnemers.
- Notitie over welke doelgroep(en) het CIP nu bedient, gericht op afstemming met andere rijksbrede ontwikkelingen – najaar 2016.

3.3. Domein Privacy

Voor Domeingroep Privacy is de invulling als volgt.

- Het uitbrengen van de eindversie (december 2016) van de publicatie "Meldplicht datalekken". Deze thematiek zal in de loop van 2017 opgaan in de AVG-implementatie.
- Grip op Privacy (GOP) documenten reviewen/verbeteren/voltooien door er gerichte acties voor te plannen en trekkers daarbij te benoemen. Planhorizon: eind mei 2017 (presentatie op de meiconferentie).
- Behoud van privacy in (nationale en internationale) ketenverwerkingen. Dit kan rechtstreeks worden gekoppeld aan de implementatie van de AVG en de ontwikkelingen rondom het Privacy Shield. Concrete actiepunten hiervoor moeten nog worden uitgewerkt.
- Visievorming rond Data Analytics. Big data en 'Internet of Things' maken vergaande profilering en geautomatiseerde beslissingen mogelijk. De domeingroep ontwikkelt een visie op de balans tussen enerzijds de mogelijkheden die ontstaan en anderzijds de grenzen in het licht van de Privacywetgeving.
- Visievorming over de privacyaspecten rond Cloud en Cyber (wat is bedoeld ??) (specificatie volgt nog).

3.4. Domein Governance & Normatiek

Voor Domeingroep Governance Governance & Normatiek is de invulling als volgt.

- De ontwikkeling en realisatie van het ambassadeurschap voor de SIVA methode.
- De werving van domeingroepleden die de ambassadeursrol op zich kunnen nemen).
- Realisatie van BIO. De domeingroep heeft op dit punt een bijdragende rol aan de interbestuurlijke werkgroep normen. Voor de BIO zijn tien thema's benoemd die in de loop van 2017 zullen worden uitgewerkt in zogenoemde "2-pagers" die in een oogopslag de essentie van het thema duidelijk maken. Dit zijn, in willekeurige volgorde:
  - Toegangsvoorziening
  - Applicatie

- Software pakketten
- Database en Storage (Opslag)
- Platformen en Servers
- Mobile Devices
- Netwerk (ExterneKoppeling)
- Housing
- Beheerprocessen
- Cloud

De domeingroep draagt bij door meeschrijven en reviewen van 2-pagers en review van door BZK opgeleverde BIR2017- en BIO-onderdelen.

- Voortzetting van de uitwerking van informatieveiligheidsthema's.
- Realisatie van ISOR. Per door CIP uitgewerkte Informatieveiligheidsthema's worden de normen/maatregelen opgenomen binnen de NORA-Wiki. Binnen NORA is voor ISOR een apart hoofdstuk opgezet. Alle uitwerkingen worden op deze wijze digitaal toegankelijk voor iedereen.
- Bewaking van het SIVA-gedachtegoed in de thema-uitwerkingen en de correcte toepassing en opname daarvan in de NORA-Wiki. (Poortwachter-functie en redactie).
- Effectmeting op het gebruik, de bruikbaarheid en de toegevoegde waarde van de producten van de domeingroep.

3.5. Domein Ketens

De domeingroep Ketens houdt zich in planperiode vooral bezig met de volgende agenda.

- Het ontwikkelen van een ketengame die in iedere willekeurige organisatie gespeeld kan worden. Net als in de eerdere game wordt als voorwaarde meegenomen dat het draaiboek volledig uitgeschreven is zodat de "spelleider" niet per definitie inhoudelijke kennis hoeft te hebben. Dit bevordert de verspreiding in hoge mate.
- Doorontwikkelen van een keten-test-dorp (KTD). In 2016 is als pilot de RNI-keten uitgewerkt. In 2017 wordt een keten uitgewerkt waarbij, naast rijksoverheid en ZBO's, ook bijvoorbeeld gemeenten betrokken worden. Een en ander is afhankelijk van de bereidheid van instanties om actief in de werkgroep te participeren bij het uitwerken van de keten.
- Creëren van draagvlak voor het KTD binnen de aangesloten organisaties en onderzoeken hoe concrete ophanging mogelijk is. Het gaat dan enerzijds om het eigenaarschap (en dus de funding) en anderzijds om het beheer van het KTD.
- Door middel van het kennisdelingsplatform, CIP-pleio, meer communiceren over het KTD.

3.6. Domein ID-fraude

Voor de domeingroep ID-fraude is het actuele en vooralsnog enige speerpunt het bepalen of en op welke wijze deze domeingroep kan voortbestaan. Dit moet begin 2017 uiterlijk duidelijk zijn. Als we doorgaan, worden ook verdere agendapunten bepaald.

3.7. Practitioners communities (PraCo's)

Voor alle practitioners communities gelden de volgende agendapunten.

- Minimaal twee practitioner bijeenkomsten in het jaar organiseren + gestructureerde digitale communicatie met de leden. (Nodig voor het in stand houden van het community-besef en het vitaal houden van de community).
- Stimuleren van gebruik en implementatie van de producten.
- Externe/interne communicatie(o.a. Pleio gebruik stimuleren).
- Practices beschikbaar maken via cip.Pleio.

- Publicaties in nieuwsbrieven.
- Aanbieden van het organiseren van collegiale toetsingen in het aandachtsgebied van de desbetreffende PraCo.

3.7.1. PraCo SSD

Specifiek voor SSD gelden nog de volgende agendapunten.

- Onderzoek naar de mogelijkheid van de ontwikkeling van een SSD-implementatiegame.
- SSD adviesraad van Manifestpartijen samenstellen.
- Extra aandacht voor het delen van practices m.b.t. SSD voor mobile applicaties. (In 2016 is dat er nog niet van gekomen).
- Upgrade van SSD, de methode met normen voor mobile en server applicaties. (Ook Agile).
- Afronding van SSD testraamwerk, uitbreiding met SSD Mobile en beschikbaar stellen.
- Zo mogelijk Internet of Things-werkgroep vormen (evt. uit doorstart SSD mobility).
- Deelname iBestuur mobility congres.
- Overzicht van SSD implementaties en referentie sites opbouwen.

3.7.2. PraCo Privacybescherming

Specifiek voor PraCo Privacybescherming gelden nog de volgende agendapunten.

- Stimuleren gebruik van de Privacy Vraagbaak voor zeer gerichte uitwisseling van binnen de organisaties levende privacy-vraagstukken.
- Upgrade privacy producten met AVG.
- Drie i.p.v. twee bijeenkomsten van de PraCo.
- Deelname iBestuur Privacy congres
- Alignment met Domeingroep Privacy vergroten.

3.7.3. PraCo Inkoop

Specifiek voor PraCo Inkoop gelden nog de volgende agendapunten.

- Thema-uitwerking IAAS en PAAS met SIVA opleveren.
- Product Veiligheid in Inkoop contracten “Grip op beveiliging in inkoopcontracten” actualiseren.
- Awareness en stimuleren van de bijdrage die inkopers/contractmanagers kunnen leveren aan Security en Privacy; promotie CIP-producten bij inkoopcommunity en bevorderen van het gebruik daarvan door inkopers en contractmanagers.
- Herijking doel, functie en bezetting van de PraCo Inkoop.

3.7.4. PraCo BIR

Specifiek voor PraCo BIR gelden nog de volgende agendapunten.

- Actuele informatieverstrekking omtrent ontwikkeling naar BIR 2017 en BIO.
- Promotie gebruik van Grip op privacy, Grip op SSD en Grip op de veiligheid in inkoopcontracten.
- Kennis ontsluiten over toepassing van GRC.

3.7.5. PraCo Awareness

Specifiek voor PraCo Awareness gelden nog de volgende agendapunten.

- Uitnodigen van interessante sprekers voor een presentatie op het domein Awareness waar de deelnemers aan de PraCo hun voordeel mee kunnen doen.

- Aan de hand van de presentaties best practices laten destilleren die ter beschikking gesteld kunnen worden aan het hele netwerk.