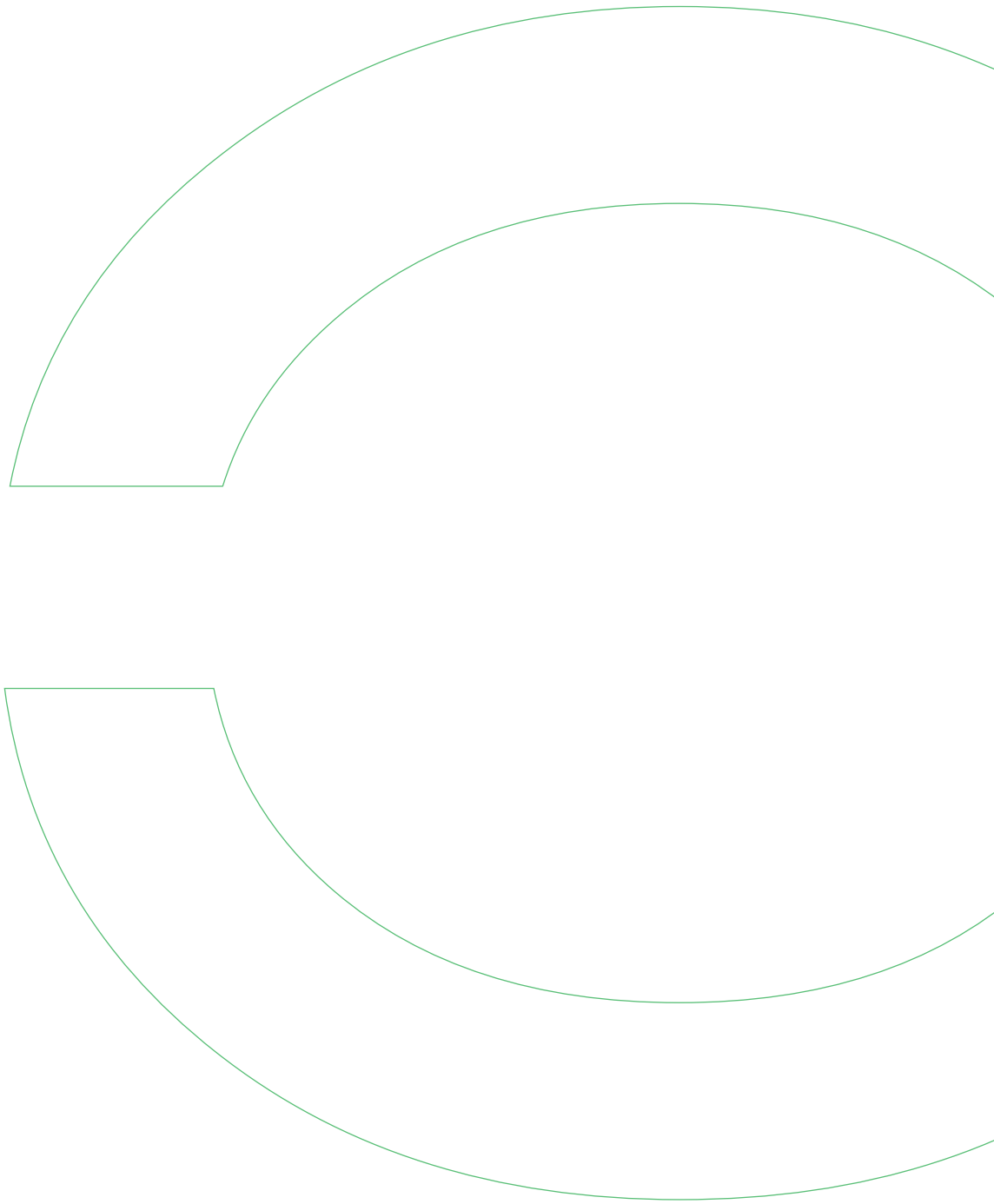
Voortgangsrapportage

Taskforce Bestuur & Informatieveiligheid Dienstverlening

februari 2013 – november 2014

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening



Inhoudsopgave

1 Instelling Taskforce BID 3

2 Aanpak langs vier lijnen 7

3 Resultaten 11

4 Bevindingen 19

Bijlagen:

I Instrumentarium voor gerichtheid en verankering informatieveiligheid 23

II Rijksoverheid 27

III ZBO 29

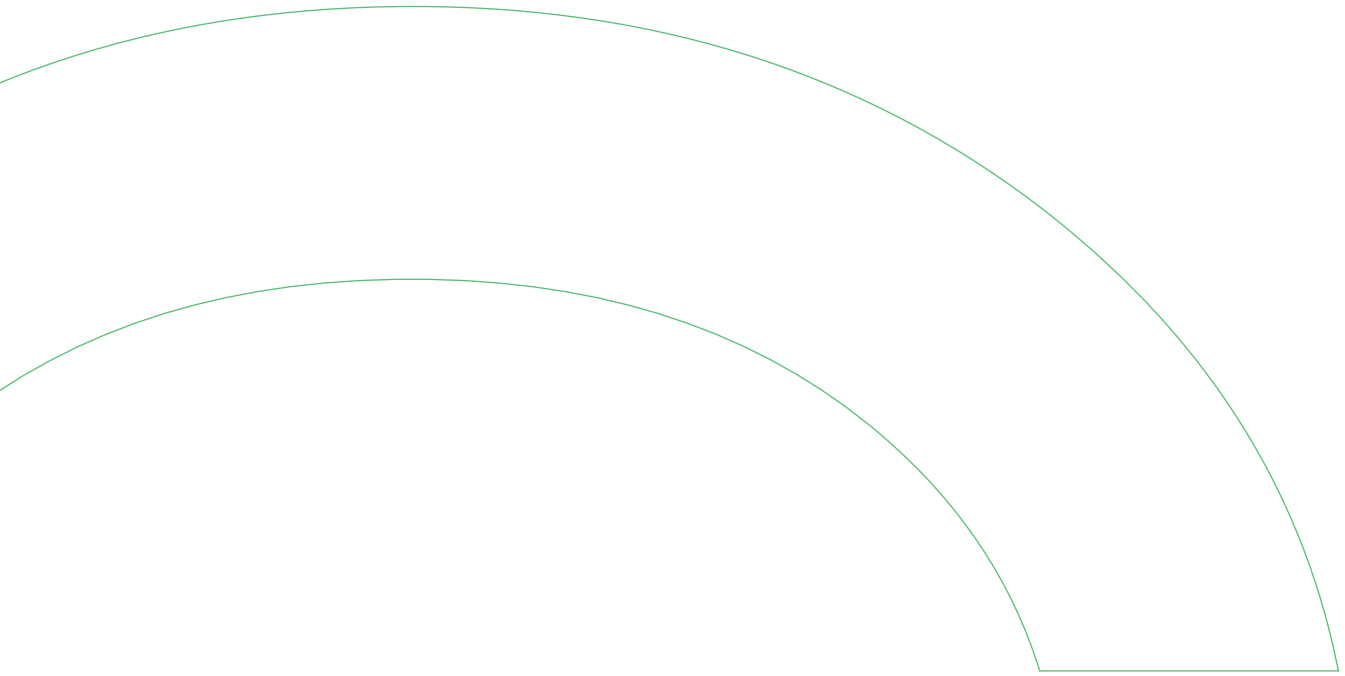
IV Provincies 33

V Waterschappen 37

VI Gemeenten 41

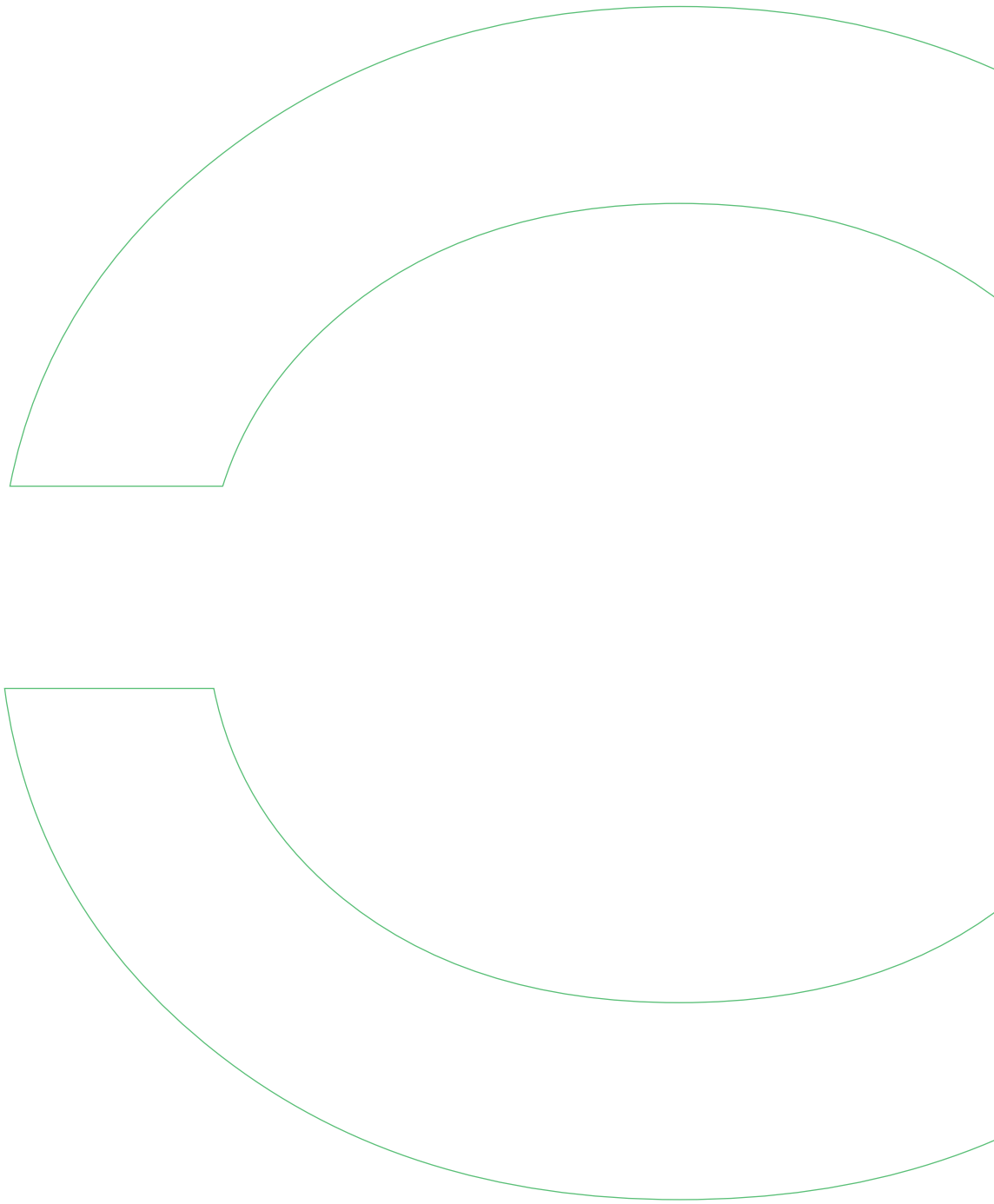
VII Rapport Onderzoeksraad voor Veiligheid - Aanbevelingen DigiNotar 45

VIII Afkortingen 47



Instelling Taskforce BID

1



1 Instelling Taskforce BID

In de Bestuurlijke Regiegroep e-overheid en dienstverlening van 13 februari 2013 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) formeel ingesteld in bijzijn van bestuurders van koepelorganisaties van de verschillende overheidslagen. De koepelvertegenwoordigers zijn het Directoraat- Generaal Organisatie Bedrijfsvoering Rijk (DGOBR), het Interprovinciaal Overleg (IPO), de Vereniging Nederlandse Gemeenten (VNG) en de Unie van Waterschappen (UvW). Met de instelling van de Taskforce BID wordt gehoor gegeven aan de aanbeveling van de Onderzoeksraad Voor de Veiligheid (OVV) om een tweejarig programma te ontwikkelen om 'bestuurders te doordringen van het belang van digitale veiligheid' en 'hen te voorzien van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie'. Met als bijkomende opdracht de voorwaarden te scheppen die noodzakelijk zijn voor overheidsorganisaties om hun digitale veiligheid systematisch te beheersen. Deze aanbevelingen zijn gedaan in het onderzoek: 'Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt'[1].

In aanloop naar de instelling van de Taskforce BID was reeds breed commitment geuit door het Rijk en de vertegenwoordigers van de koepelorganisaties (IPO, UvW en VNG), hierna te noemen medeoverheden, om naar aanleiding van het DigiNotar-incident en Lektober het thema informatieveiligheid structureel op de bestuurlijke agenda te plaatsen. Het onderzoek van de OVV versterkte dit urgentiebesef. Bij de instelling van de Taskforce BID hebben het Rijk en de medeoverheden zich gecommitteerd aan het principe van de verplichtende zelfregulering. Het komt erop neer dat overheidsorganisaties zelf verantwoordelijk zijn en blijven voor het op orde brengen en houden van informatieveiligheid in hun organisatie. Het beheer en de beheersing van informatieveiligheid moet onderdeel zijn van de informatiehuishouding van elke overheidsorganisatie. Langs die lijn, het aansporen en sturen op de eigen verantwoordelijkheid van overheidsorganisaties, wordt nadere invulling gegeven aan verbetering van de informatieveiligheid.

1.1 Eigen verantwoordelijkheid en achtergrond informatieveiligheid

De afgelopen jaren zijn binnen de overheidslagen[2] reeds verschillende ontwikkelingen in gang gezet om voor het onderwerp informatieveiligheid niet alleen de gewenste aandacht, maar ook de vereiste borging te creëren binnen overheidsorganisaties zodat het structureel de nodige aandacht krijgt. Een voorbeeld daarvan is de ontwikkeling van de verschillende baselines voor informatiebeveiliging.[3] De uitwerking en het tempo van deze ontwikkelingen verschillen sterk per overheidslaag. De Taskforce BID heeft in haar benadering voortgebouwd op reeds in gang gezette ontwikkelingen bij de overheidslagen om te komen tot een brede, gelijkwaardige versterking op informatieveiligheidsvlak binnen de overheid. Tevens benadrukt dit ook het belang van het interbestuurlijke karakter van de Taskforce BID: *"samen kom je verder"*. Uitgangspunten bij de positionering van de Taskforce BID zijn dan ook:

- ✔ Overheidsorganisaties en overheidslagen zijn en blijven zelf verantwoordelijk voor het oppakken van het thema informatieveiligheid
- ✔ Bij de start van de Taskforce BID in 2013 is uitgegaan van versterking en versnelling van de reeds lopende ontwikkelingen op informatieveiligheidsvlak.[4]
- ✔ Hiervoor is ook aangesloten bij de lopende initiatieven breed binnen de overheid op het gebied van informatieveiligheid, waar diverse partijen al enige jaren actief zijn met elk hun eigen verantwoordelijkheid en doelstelling.[5]
- ✔ Daarnaast zijn de activiteiten van de Taskforce BID gericht op hergebruik en doorontwikkeling van beschikbaar materiaal van de overheidslagen.
- ✔ Inzet daarbij is dat de activiteiten van de Taskforce BID afgestemd zijn op de reeds bereikte en te bereiken situatie binnen de overheidslagen.
- ✔ Waarbij de activiteiten samen met de verschillende belanghebbenden en samenwerkingsverbanden binnen de overheid(slagen) (door)ontwikkeld worden.

1.2 Opdracht Taskforce BID

De opdracht van de minister van BZK aan de Taskforce BID is als volgt omschreven:

1. De bewustwording te versterken van bestuur en ambtelijke top als het gaat om de eisen aan informatieveiligheid, met name ook vanuit maatschappelijke en politieke risico's.
2. Een leerstrategie uit te voeren voor een actieve gerichtheid van bestuur en ambtelijke top op adequate aanpak informatieveiligheid dienstverlening.
3. De lange termijn verankering van informatieveiligheid en gerichtheid daarop in de reguliere processen en informatieketens te versterken, waarbij gerichtheid op weerbaarheid en herstel deel zijn van die verankering. Een verplichtende vorm van zelfregulering per domein is het beoogde einddoel van die verankering.
4. De overheidsbrede coördinatie rond het stelsel van informatieveiligheid te bevorderen en te adviseren over dit stelsel.
5. Voor zover nodig aanvullend onderzoek te doen verrichten.

De uitwerking van bovengenoemde opdracht is en blijft de verantwoordelijkheid van de overheidslagen en overheidsorganisaties zelf. De Taskforce BID fungeert met name als vliegwiel, facilitator en verbinder.. De focus van de Taskforce BID ligt op organisaties uit de volgende overheidslagen: Rijk, ZBO's, gemeenten, provincies en waterschappen. In totaal 'een kleine 500 organisaties[6].

1.3 Inzet op leren

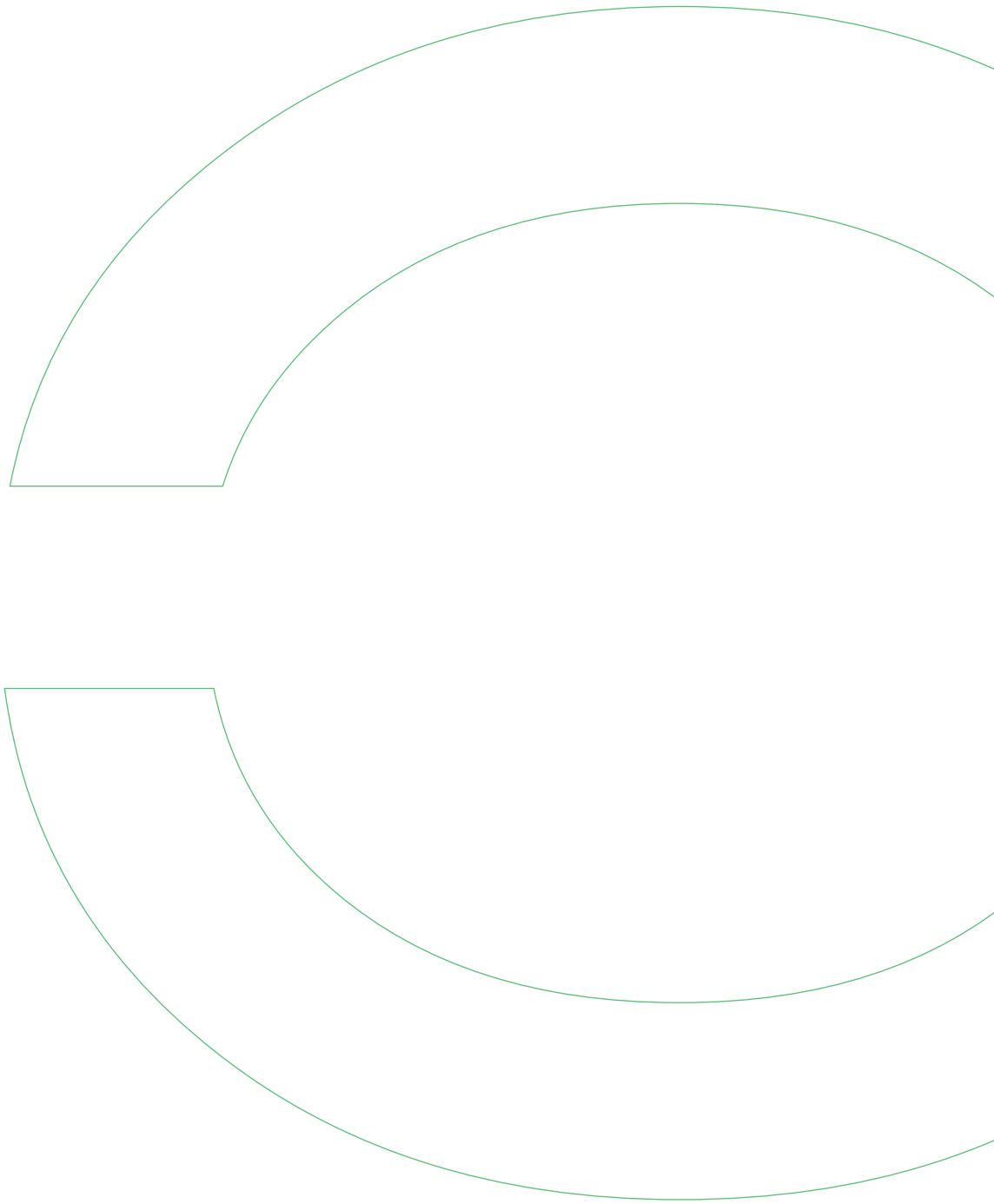
De inzet is om de verplichtende zelfregulering gedurende de looptijd van de Taskforce BID tot stand te brengen door een iteratief proces van 'leren' en 'het verankeren' op het niveau van de organisatie en de overheidslaag. De Taskforce BID heeft samen met de overheidslagen een gericht opleidingsaanbod en concrete verankeringsinstrumenten ontwikkeld en aangeboden. Daarbij is ingezet op hergebruik van bestaand en beproefd aanbod en waar nodig aangevuld met nieuw aanbod. Het doel hiervan is om met inzet van dit materiaal een zichtbare en meetbare verandering te realiseren bij bestuur en topmanagement binnen de overheidslagen op het vlak van informatieveiligheidsbewustzijn en risicobewust handelen. Het gedachtegoed wat hieraan ten grondslag ligt, wordt gevormd door organisatieleren, wat zich richt op het vergroten van een gezamenlijke organisatorische prestatie. Organisatieleren vindt plaats wanneer nieuwe kennis getransformeerd wordt in nieuwe routines van het individu naar de organisatie of omgeving en vice versa. Het helpt mensen in een organisatie verandering als een constante factor te omarmen. Het opleidingsaanbod en de verankeringsinstrumenten stimuleren en ondersteunen dit. Op deze manier verbindt organisatieleren het leren en het verankeren.

***Figuur 1**: Leerstrategie*

1 Het in 2012 verschenen rapport van de OVV: "Het diginotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt" www.onderzoeksraad.nl/uploads/items-docs/1094/Rapport_Diginotar_NL_web_def_20062012.pdf
2 De overheidslagen zijn: de rijksoverheid, de provincies, de gemeenten, de waterschappen en de ZBO's (hoewel geen formele overheidslaag, wordt er expliciet aandacht besteed aan ZBO's)
3 De baselines vormen een instrument om de informatieveiligheid van overheidsorganisaties te verbeteren en is gebaseerd op algemeen geaccepteerde kaders, zoals de NEN- ISO-27001/2 .
4 Zoals in gang gezet vanuit de VNG en de Informatiebeveiligingsdienst Nederlandse Gemeenten (IBD) (gemeenten), DGOBR(Rijksoverheid), IPO (provincies), UvW en Het Waterschapshuis (Waterschappen) , de Manifestgroep en het CIP (ZBO's).
5 Zoals Logius (als beheerder van stelselvoorzieningen) en NCSC (als Emergency en Responsteam) die al programmering op het vlak van informatieveiligheid ontwikkelden.
6 Gemeenten: 403, Provincies: 12, Waterschappen: 23, Rijk: 11 departementen incl. agentschappen en ZBO's: 30 (o.b.v. van volgende criteria: publiekrechtelijk, eigen rechtspersoonlijkheid en Kaderwet ZBO's van toepassing). Totaal: 479 organisaties.

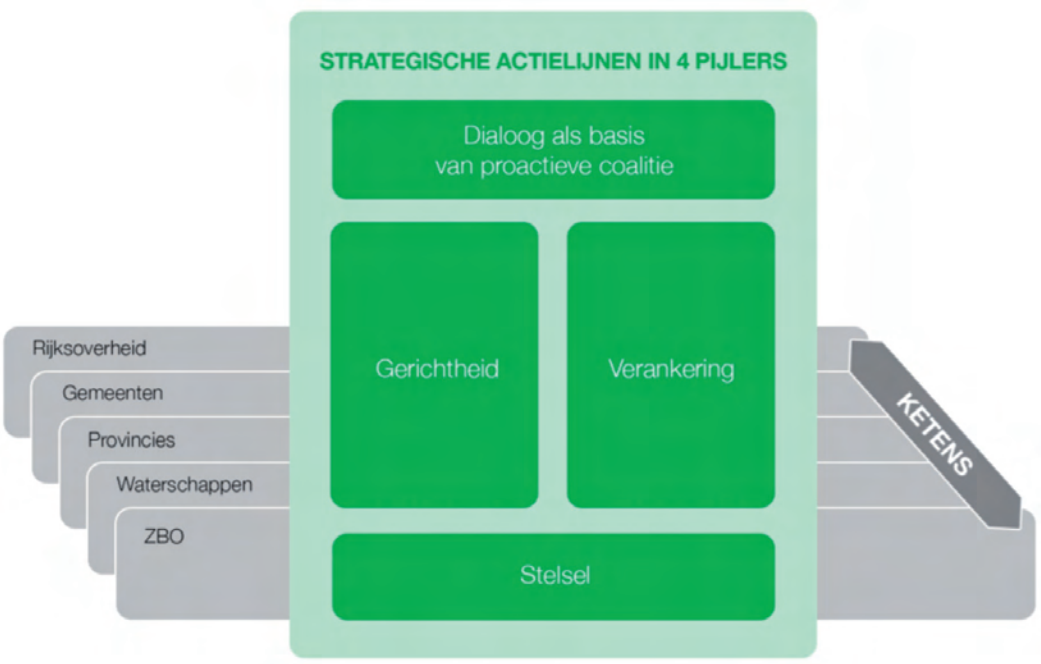
2

Aanpak langs vier lijnen



2 Aanpak langs vier lijnen

Zoals eerder gesteld, heeft de Taskforce BID de overheidslagen ondersteund bij de realisatie en verankering van verplichtende zelfregulering per overheidslaag. Hierbij is een gerichte aanpak toegepast, die in nauwe samenwerking met de koepelorganisaties, de betrokken stelselpartijen[9] en de opdrachtgever, het ministerie van BZK, tot stand is gekomen. Daarbij zijn de activiteiten, zoals eerder beschreven, uitgewerkt langs een viertal pijlers, die het kader vormen voor de activiteiten die de Taskforce BID voorziet voor de verbetering van de informatieveiligheid binnen de overheid.



***Figuur 2**: Actielijnen in vier pijlers*

2.1 Dialoog als basis voor een proactieve coalitie op informatieveiligheid

Het realiseren en voortzetten van de interbestuurlijke verbinding en dialoog is essentieel om te komen tot een sluitende aanpak. Bij een overheid die in toenemende mate onderling en met derden verbonden is via ketens, netwerken en centrale voorzieningen, is het van belang om in gezamenlijkheid te kijken naar de vraagstukken die voorliggen. Om dit te stimuleren is ingezet op het creëren van een blijvende samenwerking en dialoog tussen bestuurders en ambtelijke top van overheden en overheidsorganisaties (op diverse niveaus). Inzet daarbij is om hen blijvend te mobiliseren om binnen hun overheidslaag en organisatie(s) innovatief en proactief aan het werk te gaan op het vlak van informatieveiligheid. Daarmee leveren zij een belangrijk onderdeel voor het creëren van de benodigde borging en waarborgen op informatieveiligheidsvlak binnen de overheid. Hiervoor zijn binnen de verschillende overheidslagen zowel de bestaande vakverenigingen (bijvoorbeeld Vereniging Gemeentesecretarissen (VGS)) en gremia (bijvoorbeeld Interdepartementale Commissie Chief Information Officers(ICCIO) gebruikt, alsook dat er ingezet is op een breder informeel overleg om interbestuurlijk de noodzakelijke verbinding te kunnen realiseren op de diverse overheidslagen.

2.2 Ontwikkeling stelsel Informatieveiligheid

Langs deze lijn worden vraagstukken geadresseerd die het informatieveiligheidsbeleid doorkruisen en waarvan de overheidslagen hebben aangegeven te willen komen tot een gezamenlijke aanpak. Het tijdspad en de ambities met Digitaal 2017 en de drie decentralisaties benadrukken daarbij nogmaals de urgentie en het belang van informatieveiligheid. De uitwerking van deze vraagstukken is randvoorwaardelijk om de verplichtende zelfregulering op informatieveiligheidsvlak overheidsbreed te laten slagen. Discussies over normatiek en de daarbijhorende beleidsvraagstukken, wijze van controleren op, verantwoorden over informatieveiligheid (horizontaal en verticaal) en het inpassen van het toezichtsregime worden langs deze pijler geadresseerd. Wetgeving, het inrichten en borgen van een kennis- en leerinfrastructuur, crisisbeheersing en ketenaansturing maken hier tevens onderdeel van uit.

2.3 Instrumentarium voor gerichtheid op informatieveiligheid

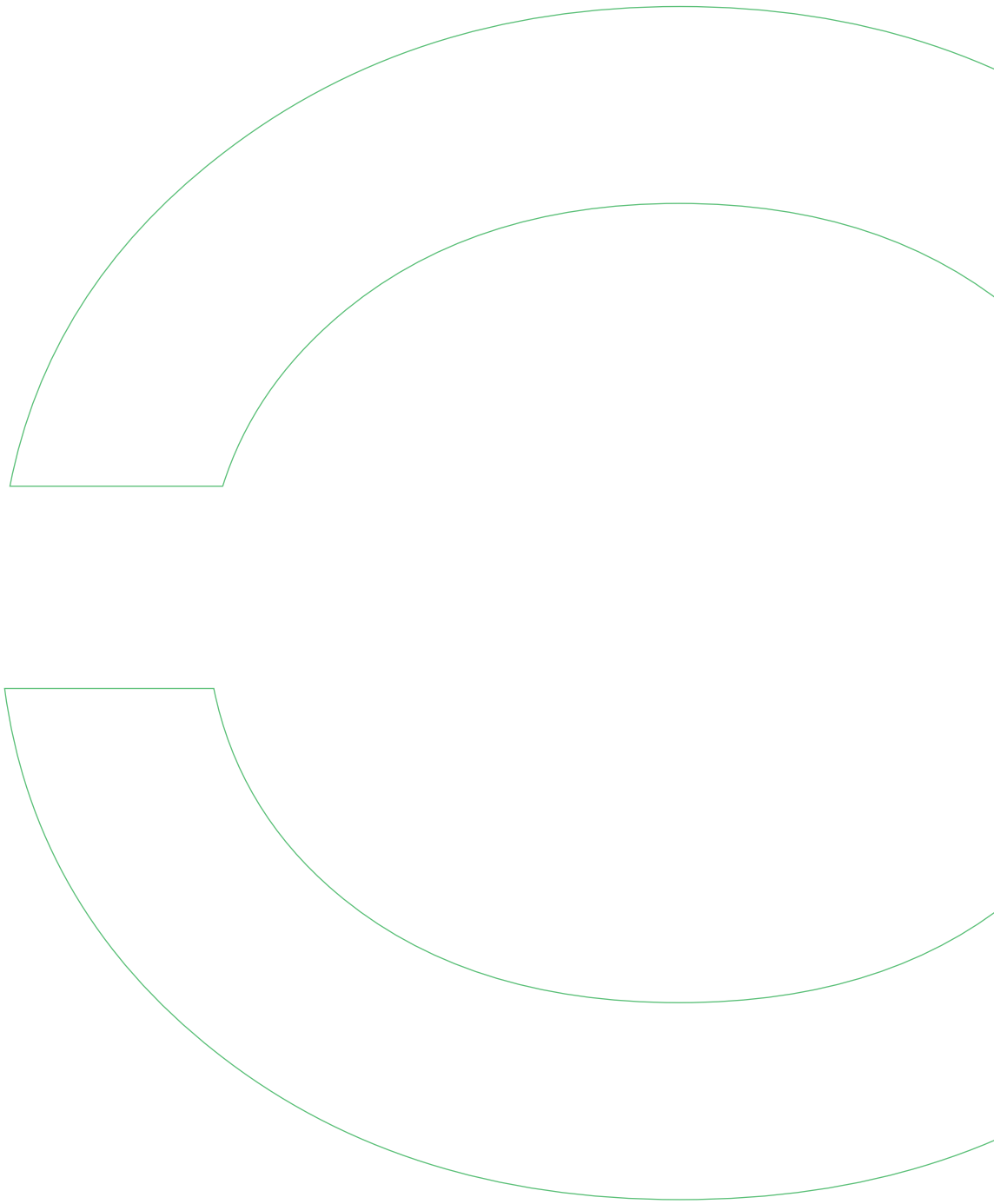
Dit betreft de ontwikkeling van het instrumentarium rond gerichtheid (leren), met als doel om verbetering te realiseren bij bestuur en topmanagement binnen de overheid op het gebied van bewustzijn en risicobewust handelen. Deze generieke instrumenten kunnen, eventueel met aanpassingen gericht op de specifieke overheidslaag, blijvend ingezet worden door koepel- en overheidsorganisaties om bewustzijn te vergroten. Daarbij gaat het om een zelftest, e-learning modules, vijf workshops, een simulatie, weerbaarheidsoefeningen en campagnes. Het instrumentarium is ingericht op basis van de binnen de Taskforce BID gehanteerde leerstrategie en dient toegankelijk en makkelijk te vinden te zijn.

2.4 Instrumentarium voor verankering van informatieveiligheid

Dit betreft de ontwikkeling van het instrumentarium om overheidsorganisaties in staat te stellen te komen tot verankering. Ook deze generieke instrumenten kunnen, eventueel met aanpassingen gericht op de specifieke overheidslaag, blijvend ingezet worden door koepel- en overheidsorganisaties om informatieveiligheid in te bedden in de organisatie en in de keten. Daarbij gaat het om een handboek incident- en crisismanagement, operationele producten voor de baselines en handreikingen, zoals factsheets, checklists, best practices en de verzameling daarvan in een toolkit.[8]

7 Organisaties die een rol of verantwoordelijkheid hebben in het vormgeven van informatieveiligheid, zoals de vakdepartementen SZW,EZ, V&J en het Nationaal Cyber Security Centrum.
8 Toolkit Informatieveiligheid Gemeentesecretarissen; deze is medio 2014 verspreid onder alle gemeentesecretarissen binnen Nederland.

3 Resultaten



3 Resultaten

Bij de start van de Taskforce BID in 2013 zijn de inspanningen vooral gericht geweest op het verkrijgen van draagvlak binnen koepelorganisaties voor de overheidsbrede aanpak op informatieveiligheidsvlak en het gezamenlijk uitwerken van een gerichte aanpak binnen deze overheidslagen. Daarbij lag in 2013 de nadruk op gerichtheid binnen bestuur en topmanagement. In 2014 is het zwaartepunt meer verschoven naar de cyclische verankering van informatieveiligheid in de processen van de verschillende overheidslagen alsook naar het stimuleren van een continue dialoog over het onderwerp tussen bestuurders en ambtelijke top binnen en tussen overheidslagen.

Onder leiding van de koepelorganisaties, ondersteund door de Taskforce BID en in samenwerking met andere partijen binnen het informatieveiligheidsdomein, zijn in de verschillende overheidslagen onderstaande resultaten behaald met betrekking tot de realisatie en verankering van verplichtende zelfregulering per overheidslaag. Deze resultaten zijn per overheidslaag nader gespecificeerd in de bijlagen.

3.1 Resultaat: Invulling Verplichtende Zelfregulering per overheidslaag

Gemeenten

Vaststelling van de Resolutie Informatieveiligheid 'Randvoorwaarde voor de professionele gemeente'[9] op 29 november 2013 tijdens de Bijzondere Algemene ledenvergadering van de Vereniging Nederlandse Gemeenten (BALV/VNG). Hiermee committeren gemeenten zich om het onderwerp informatieveiligheid op te pakken, uitgaande van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Samen met de VNG en de Informatiebeveiligingsdienst voor gemeenten (IBD)[10] is gewerkt aan de realisatie van de elementen uit de resolutie. Een van die elementen betreft het uitwerken van het toezicht op en de verantwoording over informatieveiligheid, alsook de implementatie van de BIG en de 'officiële' aansluiting bij de IBD voor gerichte dienstverlening. De IBD is ook aangesloten op het Nationaal Response Netwerk (NRN) van het NCSC voor samenwerking en response op incidenten, dreigingen en crisis.

Provincies

De Interprovinciale Baseline Informatiebeveiliging (IBI) is in 2010 vastgesteld en in gebruik bij provincies. Afspraken over de provinciale invulling van zelfregulering zijn middels het convenant 'Interprovinciale Regulering Informatieveiligheid' vastgelegd, welke is opgenomen in het reguliere besluitvormingscircuit van het IPO bestuur. Op IPO-niveau zal gerapporteerd worden over de status van informatieveiligheid middels een monitor. Daarnaast wordt gewerkt aan de ontwikkeling van het interprovinciale proces voor verantwoording en transparantie op informatieveiligheid, alsook de gezamenlijke aanpak op bewustwording. Er loopt een verkenning op samenwerking met de gemeentelijke IBD en het NRN van het NCSC, om de response bij dreigingen, incidenten en crisis beter te kunnen organiseren.

Waterschappen

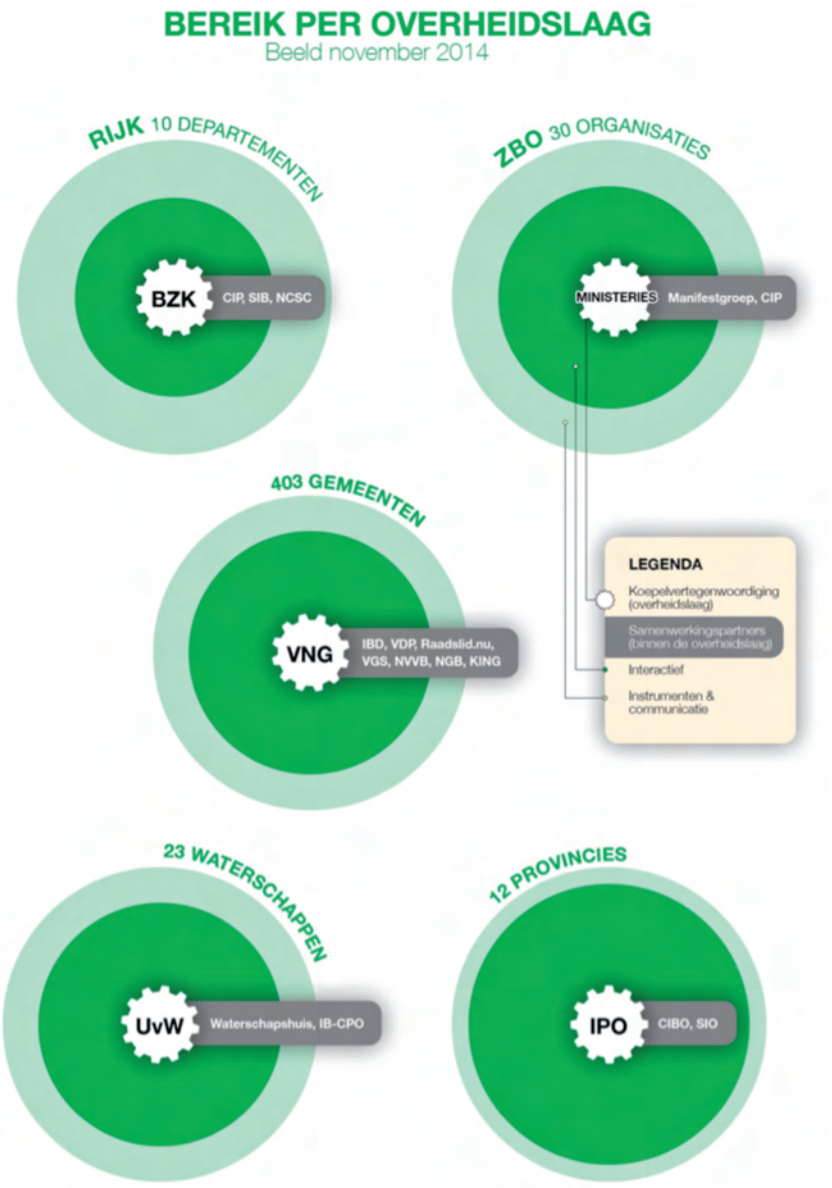
Op 2 oktober 2013 is het programmaplan 'informatieveiligheid voor de waterschappen' gelanceerd tijdens een waterschapsbrede conferentie over informatieveiligheid. Middels het programmaplan zijn afspraken gemaakt over de kaders, ambitie en governance voor verplichtende zelfregulering bij waterschappen. Dit programmaplan is bestuurlijk vastgesteld door de Unie van Waterschappen (UvW). Onderdeel hiervan is het vaststellen van de Baseline Informatiebeveiliging Waterschappen (BIWA) in 2013. Meting op de voortgang van de implementatie van de BIWA en het programmaplan verloopt via waterschapsspiegel en waterschapspeil. Op sectorniveau zijn afspraken gemaakt en geborgd over de taken en verantwoordelijkheden van elk waterschap en van de UvW ten aanzien van informatieveiligheid. Tevens loopt er een pilot om te kijken hoe de aansluiting op het Nationaal Response Netwerk van het NCSC vormgegeven kan worden, zodat ook de waterschappen de informatiedeling en response bij dreigingen, incidenten en crisis beter kunnen organiseren samen met het NCSC.

Rijksoverheid

Bij de Rijksoverheid is reeds een cyclische aanpak van de informatiebeveiliging via de PDCA-cyclus[11] van kracht, op basis van het VIR (Voorschrift Informatiebeveiliging Rijksdienst). Alle departementen werken aan de implementatie van de Baseline Informatiebeveiliging Rijksdienst (BIR), die de Rijksoverheid in september 2012 heeft vastgesteld. De Audit Dienst Rijk (ADR) voert audits uit op de invoering van de BIR vanaf 2014. Ter ondersteuning van de implementatie van de BIR zijn verschillende instrumenten ontwikkeld die ook worden ingezet voor hergebruik bij andere overheidslagen.

Zelfstandige Bestuursorganen (ZBO's)

Voor de ZBO's is in samenwerking met het ministerie Wonen & Rijksdienst/DGOBR en het Centrum voor Informatiebeveiliging en privacybescherming (CIP), een traject ingezet waarbij ZBO's en hun departementen worden uitgenodigd om het VIR en de BIR te adopteren als de leidende normenkaders. ZBO's geven hierbij invulling aan artikel 41 van de kaderwet ZBO's.[12] Daarbij wordt ook ingezet op verdergaande harmonisatie van normen tussen ketenpartijen binnen het Rijk en de ZBO's, alsook de gezamenlijke kennisontwikkeling vanuit een eenduidig normenkader voor informatieveiligheid.



***Figuur 3**: Bereik per overheidslaag, stand van zaken eind november 2014*

3.2 Resultaat: dialoog over informatieveiligheid

Tijdens het eerste Interbestuurlijk diner van de Informatieveiligheid eind 2013 en het Wereldcafe Informatieveiligheid begin 2014, is de Taskforce BID met een brede groep (ca.120 respectievelijk 60) bestuurders en topmanagers uit alle overheidslagen het gesprek aangegaan over informatieveiligheid. Specifiek over de noodzaak van samen vooruit kijken: wat komt de komende jaren aan uitdagingen op het gebied van informatieveiligheid op de overheid af? Daarbij is ook aansluiting gezocht met wetenschap en private partijen. Naar aanleiding van deze gesprekken is een Actie-Agenda Informatieveiligheid uitgewerkt met concrete acties en op te leveren producten.

Elk van de acties is tot stand gekomen in nauwe samenwerking met bestuurders en topmanagers uit de verschillende overheidslagen, vertegenwoordigers van de verschillende koepelorganisaties en inspanningen van diverse partnerorganisaties, universiteiten en het bedrijfsleven. Acties die inspelen op vraagstukken die nu voorliggen, maar ook die voor het sturen van informatieveiligheid in de toekomst van belang zijn. De acties hebben geleid tot de volgende concrete resultaten:

- ✔ Een Inspiratiebundel met essays van verschillende deskundigen
  De inspiratiebundel biedt een verdieping van het sturingsvraagstuk door in te gaan op drie kernelementen van het sturen: (1) het blijven agenderen van het vraagstuk, (2) het vormgeven van samenwerken en (3) het met elkaar blijven leren.
- ✔ Een Verkenning Informatieveiligheid Buitenland
  Voor een vijftal landen zijn de belangrijkste sturingsmechanismen voor informatieveiligheid beschreven. De verkenning biedt inspiratie om na te denken over het sturen van informatieveiligheid binnen het Nederlandse openbaar bestuur en te leren van anderen.

- ✔ Een Handreiking Cloud Computing
  Een publicatie die een toelichting geeft op Cloud Computing, inclusief de voor- en nadelen, en stuurvragen bevat die bestuurders en topmanagers houvast biedt bij gedachtevorming over de toepassing van Cloud Computing.
- ✔ Een Handreiking Goed Opdrachtgeverschap Informatieveiligheid.
  Een publicatie die concrete handreikingen biedt aan bestuurders en topmanagers bij het integreren van informatieveiligheid in projecten en aanbestedingen. De Handreiking beperkt zich niet tot de uitvraag, maar geeft ook houvast tijdens de uitvoering van ICT-projecten en aanbestedingen voor zowel opdrachtgevers, als opdrachtnemers.
- ✔ Twee kennisexpedities naar het bedrijfsleven.
  Met een selecte gezelschap bestuurders en topmanagers is een bezoek gebracht aan respectievelijk Shell (6 oktober 2014) en KPN (gepland voor 3 december 2014) om van elkaar te leren. Tijdens de kennisexpedities zijn bestuurders en topmanagers met hun evenknieën binnen het bedrijfsleven in gesprek gegaan over uitdagingen en concrete handelingsperspectieven rondom informatieveiligheid.

Tijdens het tweede Interbestuurlijk Diner van de Informatieveiligheid op 27 oktober 2014 zijn de inspiratiebundel, de verkenning en de handreikingen overhandigd aan de circa 150 aanwezige bestuurders, topmanagers vanuit de overheid en wetenschappers en afgevaardigden uit het bedrijfsleven. De resterende oplage van 1000 exemplaren is vervolgens via koepelorganisaties, kennisinstellingen en andere partners verspreid naar overheidsbestuurders en topmanagers die niet aanwezig waren op het tweede Interbestuurlijk Diner. De publicaties omvatten de gewenste inspiratie voor het verder blijven werken aan informatieveiligheid binnen het openbaar bestuur. Tegelijk is het voeding voor een brede dialoog tussen overheid, wetenschap en bedrijfsleven over informatieveiligheid.
De dialoog heeft een substantiële en inspirerende bijdrage geleverd aan gerichtheid van bestuurders en topmanagers. Deze gerichtheid heeft zich vertaald naar een actieve bijdrage aan de realisatie en de verankering van verplichtende zelfregulering op het niveau van organisaties en overheidslagen. Er is een brede basis gelegd voor een inhoudelijke dialoog over informatieveiligheid, die de koepelorganisaties en het ministerie van BZK de mogelijk biedt om ook ná het bestaan van de Taskforce BID de gerichtheid onder haar bestuurders en topmanagers te behouden en te vergroten.

3.3 Resultaten: uitwerking stelselvraagstukken informatieveiligheid

Zelfregulering is niet vrijblijvend, het vraagt om een samenhangend stelsel van normen, coördinatie van beleid en afspraken over de naleving en toetsing binnen de interbestuurlijk afgesproken kaders. Om zelfregulering op een efficiënte wijze te hanteren, is in interbestuurlijk verband gewerkt aan de doorontwikkeling van deze kaders voor informatieveiligheid. Een aantal vraagstukken zijn in dit verband geadresseerd, te weten:

a. *Normatiek*
   De overheidslagen dienen zich te conformeren aan nationale en internationale normen; deze normen zijn afgeleid van de NEN-ISO[13]-normering 27001/2. Deze normen zijn vervolgens opgenomen in de per overheidslaag (door)ontwikkelde baselines voor informatiebeveiliging, waarin maatregelen beschreven staan om een basisniveau voor informatieveiligheid te realiseren. De afgelopen periode is een interbestuurlijke dialoogfunctie ingericht, waarbinnen is afgestemd over het in samenhang doorontwikkelen van de normatiek op informatieveiligheid. Het doorontwikkelen betreft in dit geval de wijze van implementatie van de nationale en internationale normen in de diverse baselines, alsook de inhoudelijke exercitie ten aanzien van de interpretatie van de (nationale/internationale) normatiek, waar overlap in kan ontstaan, en de wijze waar hierop interbestuurlijk op kan worden samengewerkt.

b. *Toezicht*
   Met de overheidslagen zijn afspraken gemaakt over verantwoording op informatieveiligheid. Hierbij wordt aangesloten op de uitgangspunten van de Wet Revitalisering Generiek Toezicht (Wet RGT), welke een einde maakt aan de vele regelingen voor specifiek toezicht. De wet heeft als doel een afname van de bijhorende bestuurlijke drukte en beoogt helderheid te scheppen over de wijze waarop het onderlinge toezicht tussen overheden is geregeld.

   Per overheidslaag wordt momenteel een voorstel nader ontwikkeld en afgestemd over de invulling van het toezicht op informatieveiligheid.

c. *Verantwoording en Controle*
   De Wet RGT gaat uit van informatieverschaffing door middel van beleidsmonitoring, beleidsonderzoek en beleids¬evaluatie (informatie ***vooraf***) en niet door toezicht ***achteraf***.

   Verantwoording naar het eigen controlerend orgaan, zoals Gemeenteraad, Tweede Kamer, Provinciale Staten, algemeen bestuur van waterschap, over informatieveiligheid als onderdeel van de reguliere jaarverantwoording van elke overheidsorganisatie.

   Verticale verantwoording (vanuit medeoverheden richting departementen) verschilt per bestuurslaag en bestaat altijd uit een mix van zelfevaluatie en instrumenten van (onafhankelijk) toezicht. Met koepelorganisaties wordt gezamenlijk een zogeheten "Weerbaarheidsbeeld Informatieveiligheid Overheden" opgesteld, waarin wordt aangegeven wat de status en voortgang is van aanpak op informatieveiligheid binnen elke overheidslaag, alsook overheidsbreed.

Specifiek binnen het gemeentelijk domein is een pilot uitgevoerd die tot doel heeft de gemeentelijke verantwoordings- en auditlast te beperken, geheten ENSIA (Eenduidige Normatiek, Single Information en Audit).

d. *Kennisinfrastructuur:*
Het gehele stelsel van informatieveiligheid bij de overheid wordt ondersteund door samen te werken ten aanzien van kennisontwikkeling, het aanbieden van opleidingen en het van elkaar te leren. Met de partijen binnen dit stelsel wordt gewerkt aan afspraken over kennisdeling en het waar mogelijk creëren van (een gezamenlijk) opleidingsaanbod. Inzet is om voor de afronding van de Taskforce BID te komen tot afspraken voor het optimaal laten functioneren van de kennis- en leerinfrastructuur, zodat de benodigde kennis en expertise voor verplichtende zelfregulering in 2015 en verder op peil blijft.

e. *Ketens en vernetwerkte dienstverlening:*
Bijna alle overheidsdienstverlening komt tot stand via informatieverbindingen tussen verschillende (overheids)organisaties. Deze informatieverbindingen raken steeds meer met elkaar verknoopt. Aan de Taskforce BID is gevraagd de specifieke problematiek te verdiepen die hiermee gepaard gaat, zodat handelen mogelijk wordt (zowel op organisatie- als op stelselniveau). De Taskforce heeft hiervoor breed met het veld gesproken, zowel met CIO's, als met ervaringsdeskundigen uit diverse overheidslagen en met de wetenschap. Geconstateerd is dat er specifieke vraagstukken gepaard gaan met het feit dat informatie in verbindingen tot stand komt. Deze problematiek is geïnventariseerd en zijn vanuit de praktijk drie perspectieven geabstraheerd om hier in de nabije toekomst beter op te kunnen sturen. Naast het verdiepen van de problematiek en het verdiepen van oplossingsrichtingen, zijn handreikingen en workshops ontwikkeld en voorzien voor overheidsorganisaties, om meer grip te krijgen op het vraagstuk van de ketens en vernetwerkte dienstverlening.

f. *Crisisbeheersing:*
Het is van groot belang dat overheidsorganisaties de crisisbeheersing in de eigen organisatie ingericht hebben, met de daarbij behorende crisis - en continuïteitsplannen. Ter ondersteuning hiervan heeft de Taskforce BID generieke handboeken en een generieke informatieveiligheidsoefening ontwikkeld om de crisisplannen te kunnen oefenen. Daarnaast is met de koepelorganisaties gewerkt aan de aansluiting op het Nationaal Respons Netwerk (NRN) van het NCSC. De Informatiebeveiligingsdienst voor gemeenten (IBD) is reeds partner in het NRN. Vanuit provincies en waterschappen lopen nu pilots voor aansluiting op het NRN.

g. *Wetgeving:*
Er is onderzoek gedaan naar wet- en regelgeving op informatieveiligheid, die verplichtende zelfregulering ondersteunt en de interbestuurlijke inzet bekrachtigd. Wetgeving is hierbij ondersteunend aan de reeds ingezette acties van de overheidslagen. Momenteel wordt door het ministerie van BZK inzichtelijk gemaakt aan welke wettelijke grondslagen overheidsorganisaties zich reeds dienen te conformeren en hoe deze wettelijke grondslagen samenhangen. Een voorstel tot wenselijke aanpassingen in wet- en regelgeving wordt momenteel nader verkend. Dit voorstel zal naar verwachting medio 2015 worden afgestemd met de verantwoordelijke departementen.

h. *Coördinatie:*
Met de instelling van de Nationaal Commissaris Digitale Overheid (NCDO) zal de governance er anders uit komen te zien. Dit kan zijn weerslag hebben op het huidige interbestuurlijk samenspel op informatieveiligheid. De nadere invulling, impact op en wijze van organiseren op informatieveiligheid zal worden afgestemd met de NCDO. Deze afstemming vindt mogelijkerwijs plaats in het najaar van 2014.Hierna worden de contouren duidelijk en zal informatieveiligheid in de governance en aanpak van de NCDO een (mogelijke) plek krijgen.

3.4 Resultaten: Generiek aan bod

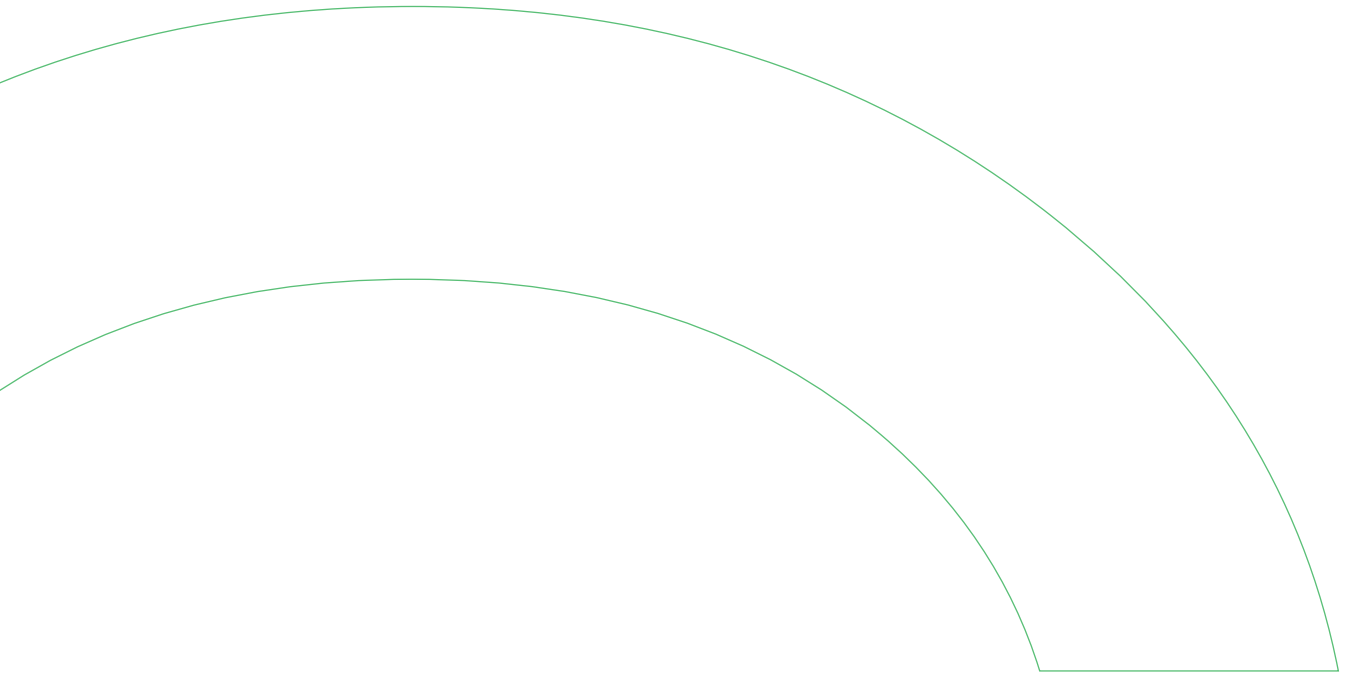
Om de beoogde mobilisatie te bereiken heeft de Taskforce BID ingezet op een middelenmix omde doelgroepen via verschillende kanalen kennis kunnen te laten nemen van de vraagstukken rondom informatieveiligheid, alsook hun rol en verantwoordelijkheid in deze. Uitgangspunt daarbij is om zoveel als mogelijk in te zetten op een generiek aanbod, door bestaand aanbod beschikbaar te stellen voor alle overheidslagen of nieuw generiek aanbod te ontwikkelen. Waar gepast zijn kleine specifieke wijzigingen t.b.v. de aansluiting op en herkenning binnen de verschillende overheidslagen doorgevoerd.

Het generieke aanbod is zo opgesteld dat overheidslagen dit zelfstandig blijvend kunnen inzetten. Via een train-de-trainer concept zijn geïnteresseerden van alle overheidslagen in staat gesteld om kennis te nemen van het aanbod en de inzet daarvan.

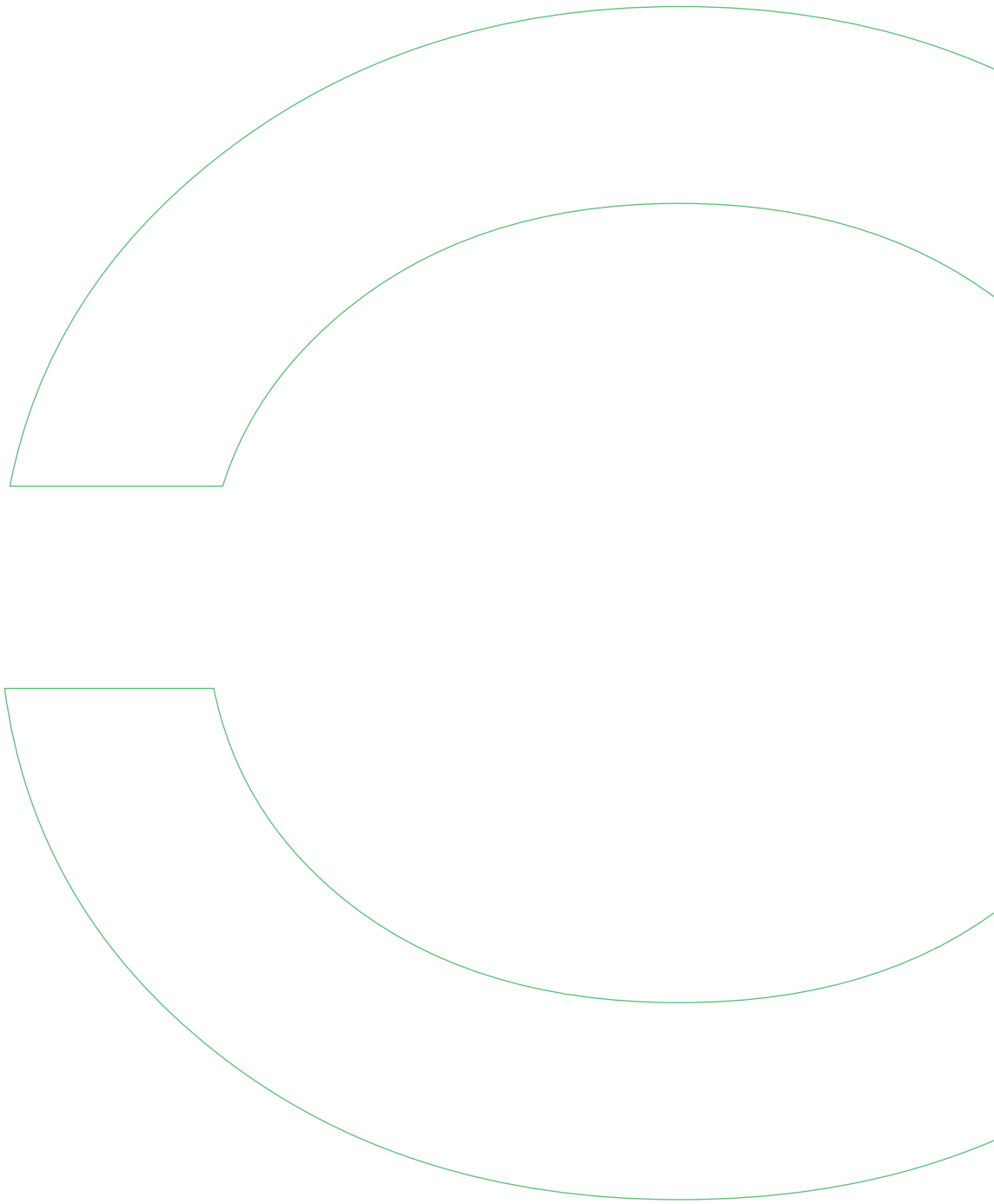
Er is een deelsite informatieveiligheid op pleio.nl ingericht om bestaand aanbod binnen de overheid en het ontwikkelde generieke aanbod te delen met alle overheidslagen. Het dient als een community voor bewustzijn en risicobewust handelen op het gebied van informatieveiligheid.

***Figuur 4**: Inzet middelenmix*

9 Nadere informatie over de overige elementen uit de Resolutie Informatieveiligheid is te vinden op www.vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid
10 De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen. Eén van de doelen van de IBD is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. Het vormt tevens de verbinding met het NCSC.
11 PDCA-cyclus staat voor Plan Do Check Act
12 In Art. 41 lid 1 Kzbo is een algemene zorgplicht ten aanzien van informatiebeveiliging opgenomen: "Een zelfstandig bestuursorgaan draagt op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorg voor de nodige technische en organisatorische
13 ISO staat voor Internationale Organisatie voor Standaardisatie



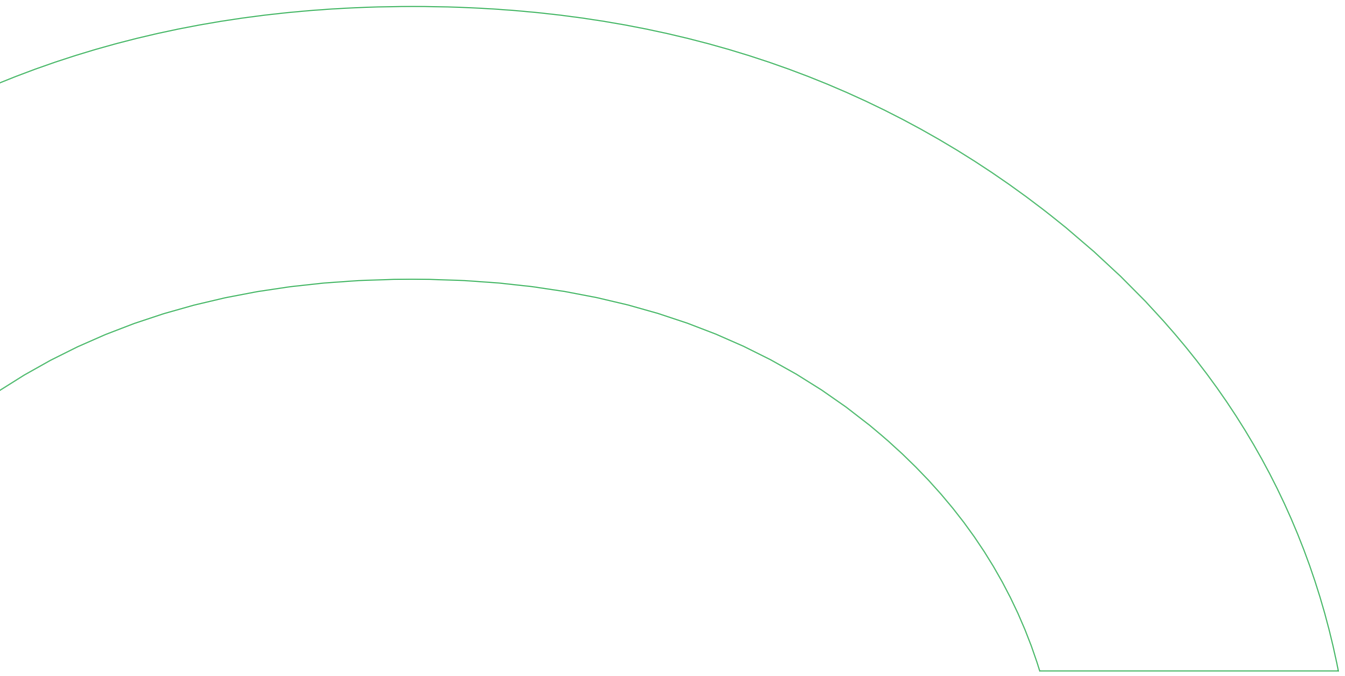
4 Bevindingen



4 Bevindingen

De Taskforce BID heeft ingezet op organisatieleren en leren van elkaar als basis voor een gedegen sturing op informatieveiligheid. Daarbij zorgt de brede aanpak voor een transformatie op dit thema: het is meer dan de som der delen. In dat kader is ook een aantal bevindingen waargenomen die het belang van het thema, de gekozen aanpak en de interbestuurlijke samenwerking bekrachtigen.

- De urgentie en complexiteit van het thema informatieveiligheid in het licht van huidige samenleving wordt door alle overheidskoepels en de daaraan verbonden overheidsorganisaties onderkend.
- De uitgangspunten van zelfregulering en organisatieleren worden daarbij als wenselijk beschouwd, om te komen tot sturing op risico's en niet het afwerken van vinklijstjes.
- Het belang van samenwerking om tot een sluitende gezamenlijke aanpak te komen binnen het openbaar bestuur, wordt door alle overheidskoepels en de daaraan verbonden onderkend.
- Het belang van horizontale en verticale verantwoording wordt door alle partijen onderschreven.
- Verdergaande samenwerking en hergebruik op het vlak van de uitwerking van rollen en verantwoordelijkheden, harmonisering van normatiek e.d. zorgt voor meer doelmatigheid in de aanpak.
- De adoptie van het thema informatieveiligheid door bestuurlijke boegbeelden (sponsoren) draagt bij aan het draagvlak en commitment vanuit overheidsorganisaties en overheidslagen (de aanpak vanuit de Actie- Agenda Informatieveiligheid).
- Door daarbij ook in te zetten op verbinden van de verschillende bestuurlijke boegbeelden, ontstaat al snel een gemeenschap die verder wil en kan kijken dan alleen de eigen organisatie of overheidslaag.
- Voor de aanpak van de ketenrisico's op informatieveiligheid, dienen organisaties als eerste de eigen zaken op orde te hebben, willen we kunnen sturen op informatieveiligheid over de ketens heen.
- Daarbij verlicht interbestuurlijke harmonisatie op baselines de ketenproblematiek, door het hanteren van gelijkwaardige begrippenkaders en het hanteren van eensluidende operationele maatregelen.
- Waarbij wel altijd rekening gehouden dient te worden met de voor de overheidslaag specifieke situatie; de dienstverlening van waterschappen is bijvoorbeeld wezenlijk anders dan de dienstverlening van gemeenten.
- De aanjagende en faciliterende rol van de Taskforce maakt het mogelijk om die onderwerpen op te pakken, waarvan de belangen verder reiken dan de eigen organisatie of overheidslaag. Deze samenwerking op het niveau van 'het gehele stelsel' heeft een duidelijke meerwaarde die ook na het opheffen van de taskforce nastrevenswaardig is.
- Daarmee ontstaat ook de ruimte om ontwikkelingen te identificeren en daar verder uitwerking aan te geven, voorbeelden zijn ketenproblematiek, normatiek, kennisinfrastructuur nieuwe technologiën.



BIJLAGE

Instrumentarium voor gerichtheid en verankering informatieveiligheid

I Instrumentarium voor gerichtheid en verankering informatieveiligheid

De TaskforceBID wil overheden handvatten bieden om in control te komen en te blijven, zodat zij veilige digitale dienstverlening en bedrijfsvoering kunnen blijven garanderen. Hierbij richt de Taskforce BID zich op het vergroten van de gezamenlijke organisatorische prestatie: het verbeteren van het niveau van informatieveiligheid binnen een overheidslaag en tussen overheidslagen, zodat de gehele overheid 'in control' is op informatieveiligheid. De bijbehorende aanpak loopt van nadruk op persoonlijke bewustwording en het verkrijgen van inzicht en kennis, naar verankering binnen organisatie en (bestuurlijke) omgeving, verankering binnen overheidslaag en uiteindelijk verankering breed binnen de overheid. Daartoe is instrumentarium ontwikkeld om bestuurders en topmanagement bewust en handelingsgericht te maken en te ondersteunen bij het stimuleren van organisatieleren op gebied van informatieveiligheid. Het instrumentarium bestaat uit workshops, leerinstrumenten en verankerinstrumenten.

De Taskforce BID heeft in 2013 5 workshops en instrumenten ontwikkeld samen met overheidsorganisaties. Deze workshops en instrumenten zijn getoetst in pilots bij verschillende overheden en meerdere keren ingezet tijdens conferenties en events en/of op verzoek van individuele overheidsorganisaties of vakverenigingen.

Uitgangspunt bij het leer- en verankeraanbod is dat het generiek van opzet is. Waar nodig is maatwerk per overheidslaag mogelijk. Zo zijn er afzonderlijke cases per overheidslaag uitgewerkt ten behoeve van de herkenbaarheid. Daarbij is de opzet en de boodschap van de workshop gelijk gehouden om de uitwisselbaarheid en daarmee de verbinding tussen de overheidslagen te behouden.

Per overheidslaag is nauwkeurig bepaald hoe en wanneer het aanbod ingezet kon worden afhankelijk van de behoeften vanuit de overheidslaag zelf. Zo is er bij gemeenten veel via de vakverenigingen georganiseerd, terwijl er voor de Rijksoverheid per departement bekeken is waar de behoeften lagen.

I. Ontwikkeld instrumentarium

Leeraanbod:

- Zelftest informatieveiligheid voor bestuurders
- Informatieve filmpjes met oproep bestuurders
- Simulatiegame
- Confrontatieworkshop met animatiefilms per overheidslaag
- Confrontatieworkshop Ketens
- Dialoogsessies
- Risicobewustzijn-sessie
- Procesworkshop
- Procesworkshop Ketens
- Verankersessie
- Stuurvragen voor bestuurders en topmanagers
- Keteninformatieveiligheidstest
- E-learning modules[14]
- Generieke bewustwordingscampagne iBewustzijn Overheid
- App iVeiligheid[15]

Verankeraanbod

De Taskforce BID heeft in samenwerking met de overheidslagen en de werkgroep Ketens een aantal handreikingen zoals stuurvragen, checklists, een handboek en oefeningen ontwikkeld en verankeringsinstrumenten ontwikkeld. Het gaat hier om:

- Factsheet Risico's
- Checklists Informatieveiligheid
- Stuurvragen Informatieveiligheid
- Stuurvragen Informatieveiligheid Ketens
- Risicoanalyse systematiek: MAPGOOD voor andere overheden;
- Handreikingen Informatieveiligheid in P&C cyclus;
- Instrumenten voor de ketentoolkit gebaseerd op ARM en TTISC;
- Handboek incident- en crisismanagement;
- Informatieveiligheidsoefening.

Specifiek is door IBD, met ondersteuning van de Taskforce, een reeks van 40 operationele handreikingen ontwikkeld voor gemeenten, waaronder:

- Format GAP-analyse
- Voorbeeld beleid
- Stappenplan Implementatie BIG
- Geheimhoudingsverklaring BIG
- Voorbeeld Incident Management en responsebeleid
- Handreiking dataclassificatie
- Handreiking screening personeel
- Handreiking Patchmanagement voor gemeenten
- Voorbeeld toegangsbeleid
- Voorbeeld anti-malware beleid
- Handreiking Cloud computing
- Handreiking Mobile Device Management
- Handreiking Mobiele gegevensdragers
- Voorbeeld hardening beleid voor gemeenten
- Handreiking Backup en recovery

25 van deze producten zijn vervolgens geschikt gemaakt voor andere overheidslagen.

Door BZK/DGOBR ontwikkeld, met ondersteuning van de Taskforce, te behoeve van de rijksoverheid en ZBO's:

- Quickscan BIR
- Risicoanalyse systematiek: IRAM voor rijksoverheid;

II. Wijzen van aanbieden instrumentarium:

Per overheidslaag is bekeken hoe en wanneer het aanbod het best aangeboden en geborgd kon worden:

- Als start van een dialoog (vaak in verkorte vorm);
- Als losse workshop of instrument;
- Via een leerkring als leerprogramma;
- Als onderdeel van een masterclass;
- Als campagne iBewustzijn Overheid (combinatie van e-learning/zelftest, workshop en communicatiecampagne en iVeiligheidsapp);
- Als toolkit voor bestuurder of topmanager;
- Als aanvulling of uitbreiding van een bestaande mediamix of toolkit bij een overheidsorganisatie of ander platform.

III. Borgingsinstrumenten

Borging van het ontwikkeld instrumentarium gaat via verschillende lijnen.

Voor de overdracht van het instrumentarium voor verankering wordt in het najaar van 2014 ingezet op:

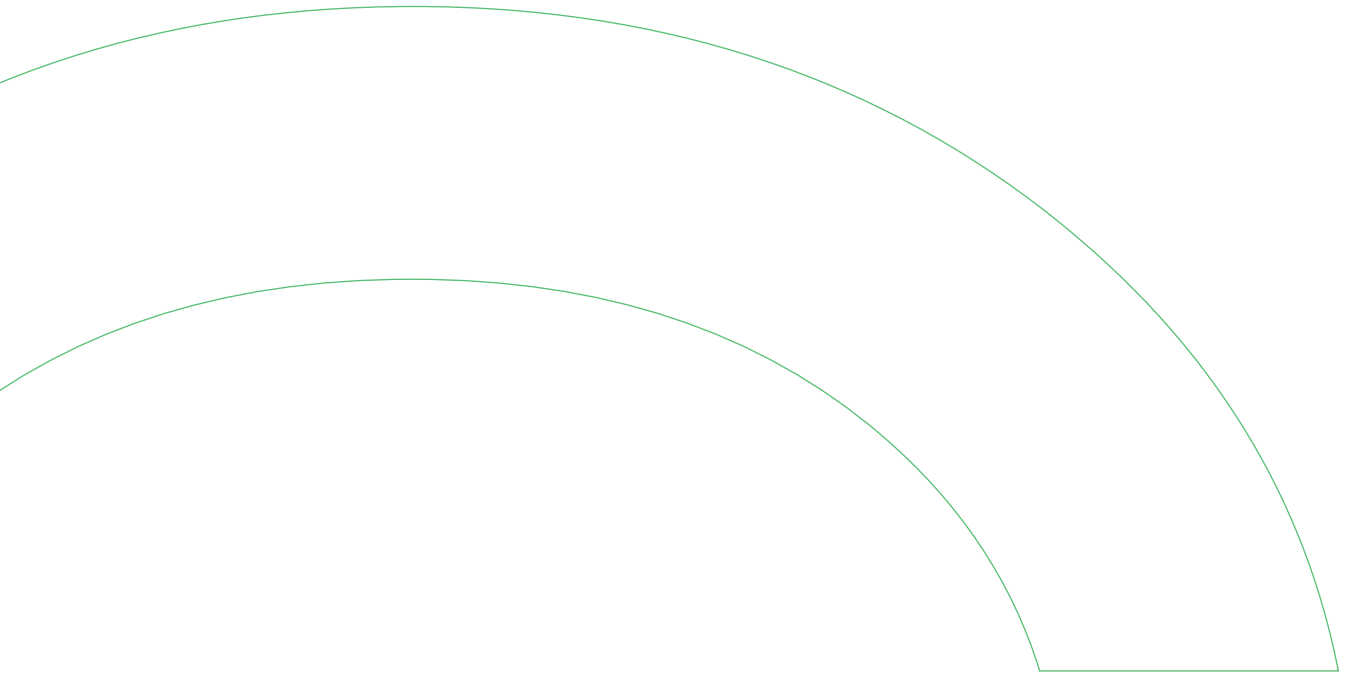
- Deelsite informatieveiligheid op pleio.nl waar het aanbod ter beschikking wordt gesteld aan management en medewerkers binnen overheidsorganisaties
- Het faciliteren van kennisuitwisseling op deze deelsite (good practices)
- Afspraken met koepels over inzet en eigenaarschap van het instrumentarium
- Afspraken met koepels over (interbestuurlijke) doorontwikkeling en beheer van het instrumentarium

Voor overdracht van het leeraanbod wordt in het najaar van 2014 ingezet op:

- Trainerskit bestaande uit flyers, draaiboeken en teachingplannen
- Train-de-trainer sessies voor Rijksoverheid en ZBO's
- Train-de-trainer sessies voor de mede-overheden
- Ondersteuning van e-learning omgeving voor iBewustzijn Overheid aan VNG academie

14 De campagne iBewustzijn Overheid is gelanceerd tijdens de Alert Online campagne van 27 oktober 2014 tot 6 november 2014. Alert Online.nl is een campagne van en voor overheid en bedrijfsleven. Als centraal platform in de campagne brengt de website acties, initiatieven en projecten onder de aandacht van organisaties die samen de oproep doen om veilig en bewust te internetten. Door gezamenlijk tijdens de campagneperiode de krachten te bundelen is het de bedoeling om een sterke impuls te geven aan het cyber security bewustzijn in Nederland.

15 De Taskforce BID heeft een app iVeiligheid ontwikkeld op basis van elementen uit de bestaande instrumenten, om gerichtheid te blijven stimuleren op een leuke en interactieve manier. Deze app is gelanceerd op 23 september 2014 en verschenen in zowel de Google Play Store (Android) als de iTunes Store (iOS-Apple) voor smartphones en tablets.



BIJLAGE

Rijksoverheid

II

II Rijksoverheid

I. Organiseren verplichtende zelfregulering Rijksoverheid

De Rijksoverheid kende reeds voor de start van de Taskforce BID, het Beveiligingsvoorschrift Rijksdienst, het Voorschrift Informatiebeveiliging Rijksdienst (VIR), het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) en de Baseline Informatiebeveiliging Rijk (BIR). Dit is voor de rijksoverheid ook de basis waarlangs de Taskforce BID samen met DGOBR, ICCIO en een subcommissie van de ICCIO op gebied van Informatie Beveiliging en Privacy (SIB) werkt in een drietal lijnen.

1. De Taskforce BID steunt initiatieven die de implementatie van de BIR en de gerichtheid daarop van het management kunnen versterken.
2. De Taskforce BID ondersteunt bij het opvolging geven aan de acties, zoals die uit de audit van de BIR volgen.
3. De SIB en Taskforce BID werken samen aan de uitwerking van een aantal interbestuurlijke opgaven, zoals ketens, single audit, breed opleidingsaanbod en het ter beschikking stellen van best practices.

II. Gerichtheid Rijksoverheid

Binnen de rijksoverheid is de afgelopen jaren al het nodige opgepakt rondom bewustwording op informatieveiligheid. De behoefte was dan andersoortig dan binnen de overige overheidslagen. In samenwerking tussen de Taskforce BID en de ICCIO/SIB is een “Roadshow” ontwikkeld, waarbij de lijnmanagers worden benaderd door de ICBR leden om hen, in samenwerking met de CIO’s, bewust te maken op het gebied van Informatieveiligheid. De Roadshow is een interactieve bijeenkomst om met bestuurders, topmanagers en lijnmanagers in gesprek te gaan over informatieveiligheid en hun verantwoordelijkheid daarin. Deze Roadshow heeft in het najaar van 2014 gelopen bij een aantal departementen.

DGOBR heeft daarnaast het programma iBewustzijn Rijk ontwikkeld, deels met ondersteuning van de Taskforce, om medewerkers bij de rijksoverheid bewust te maken van de vraagsstukken rondom informatieveiligheid. Dit programma zal binnen de gehele rijksoverheid ingezet worden. In dit kader is ook een opleidingsmodule informatieveiligheid voor bestuurders in de e-learning omgeving opgenomen. Rondom de Alert Online campagne najaar 2014 is er bij verschillende departementen aandacht geweest voor de lancering van iBewustzijn Rijk. Tijdens deze kick off-bijeenkomsten zijn het materiaal en de activiteiten van de Taskforce ook ruim aan bod gekomen.

III. Verankering Rijksoverheid

Aan een adequate verankering van informatieveiligheid heeft de Taskforce bijgedragen door het mede ontwikkelen van instrumenten voor risicomanagement. Zo is een quickscan BIR ontwikkeld waarmee vastgesteld kan worden of de BIR voldoende beveiliging biedt voor een processen met bijbehorend(e) informatiesyste(e)m(en). Ook is een train-de-trainer-cursus voor de quickscan BIR ontwikkeld en georganiseerd (acht cursusgroepen, 100 deelnemers). Voor processen die boven het beveiligingsniveau van de BIR uitstijgen wordt een aanvullende risicoanalysemethodiek ontwikkeld gebaseerd op IRAM (conceptversie voor gebruik is met een pilot vastgesteld).

IV. Bereik Rijksoverheid

Voor de Rijksoverheid is een bijdrage geleverd aan een aantal grote congressen door middel van presentaties en workshops. De nadruk heeft echter gelegen op het creëren van meer draagvlak bij enerzijds relevante gremia als ICBR, ICCIO en SIB en anderzijds bij de departementen zelf. Voor de departementen is dit gedaan door middel van organisatie van de Roadshows en middels ondersteuning van de implementatie van het programma iBewustzijn Rijk.

BIJLAGE

ZBO

III

III ZBO

I. Organiseren verplichtende zelfregulering ZBO

Voor de ZBO's is, in samenwerking met het ministerie Wonen & Rijksdienst/DGOBR en het Centrum voor Informatiebeveiliging en Privacybescherming (CIP), een traject ingezet waarbij ZBO's en hun departementen worden uitgenodigd om het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijk (BIR) te adopteren. Hiermee dwingen de ZBO's, indien ze nog geen normenkader hebben, zich tot het inrichten van processen die leiden tot grotere beheersing op het vlak van informatieveiligheid. De ZBO's die al wel een normenkader hebben, committeren zich door adoptie van VIR en BIR aan een gemeenschappelijke basis, die zij kunnen doorvertalen naar hun eigen situatie. Dit betekent bijvoorbeeld dat wanneer ZBO's gehouden zijn aan aanvullende (inter-)nationale wet- en regelgeving, zij aanvullende maatregelen doorvoeren bovenop de BIR.

ZBO's geven hierbij invulling aan artikel 41 van de kaderwet ZBO's.[16] Daarbij wordt ook ingezet op verdergaande harmonisatie van normen tussen ketenpartijen binnen het Rijk en de ZBO's, alsook de gezamenlijke kennisontwikkeling vanuit een eenduidig normenkader voor informatieveiligheid.

In een rondgang is informatieveiligheid in het ZBO-landschap nader verkend. In deze verkenningsronde is gekeken naar de stand van zaken omtrent informatieveiligheid bij de desbetreffende organisatie, het bewustzijn bij bestuur, de relatie met het kerndepartement en de vraag welke behoeften er op dit thema leven. De resultaten van de verkenningsronde zijn verwerkt in een rapportage, met daarin ook een aantal aanbevelingen over wat er op korte termijn opgepakt zou kunnen worden in termen van nader onderzoek, het beleggen van rollen en verantwoordelijkheden en de borging. De rapportage is onder de betrokken ZBO's, departementen, het CIP en de ICCIO/SIB verspreid.

II. Gerichtheid ZBO

Zowel met de rondgang als in individuele gesprekken is met het bestuur en management van de grote en kleinere ZBO's gesproken over het belang van informatieveiligheid en de wijze van sturing daarop. Daarnaast is met de kleine ZBO's de verbinding gezocht via Klein-Lef[17] om zo ook met hen gericht het gesprek te voeren.

III. Verankering ZBO

Voor de verankering van informatieveiligheid is vooral aansluiting gezocht bij de werkwijze binnen de rijksoverheid:

- De gestandaardiseerde methode voor risicoanalyse, inclusief een quickscan BIR is ook beschikbaar voor ZBO's. Ook train-de-trainer-sessies voor de quickscan kunnen worden gevolgd door de ZBO's.
- Er is een impactanalyse BIR uitgevoerd om de consequenties van de implementatie van de BIR te kunnen bepalen bij ZBO's. Deze quickscan resulteert in een handreiking voor ZBO's hoe zij om kunnen gaan met implementatie van de BIR.

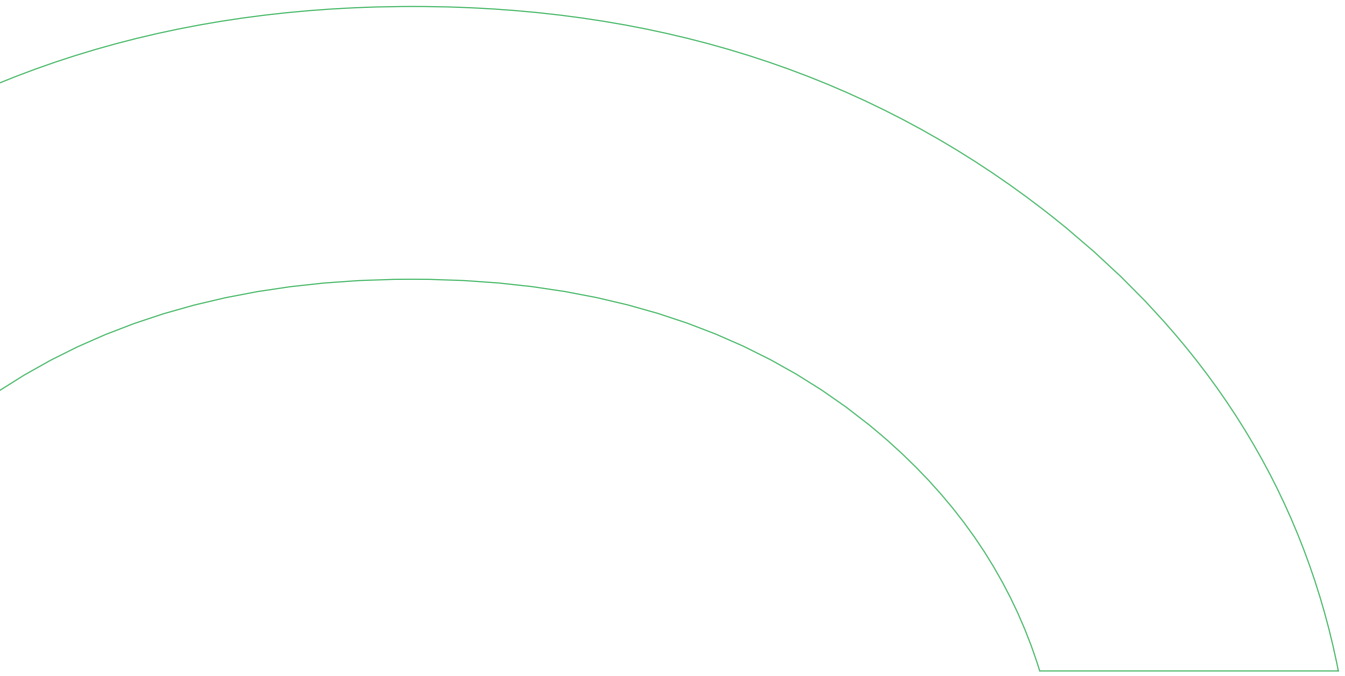
Ten behoeve van de verankering van informatieveiligheid heeft de Taskforce naast het reguliere aanbod een aantal ZBO-specifieke producten opgeleverd. Deze producten zijn fysiek verspreid tijdens eigen bijeenkomsten en bijeenkomsten van onze partners. Waar mogelijk zijn deze producten ook digitaal aangeboden via de website van de Taskforce BID, de deelsite informatieveiligheid op Pleio en via de websites van onze partners. Het gaat hierbij om:

- Specifieke factsheets /handreikingen voor doelgroepen binnen de ZBO's (bestuurders en (lijn)managers). Deze factsheets en handreikingen gaan in op de specifieke stuurvragen die vanuit de desbetreffende rol relevant zijn en het ondersteunde leeraanbod van de Taskforce BID. Deze handreikingen helpen bestuurders en managers om zich bewust te zijn van de risico's en kwetsbaarheden, alsook om procesmatig de goede vragen te kunnen stellen.
- De binnen het gemeentelijke domein ontwikkelde "Toolkit Informatieveiligheid Gemeentesecretarissen" wordt in het najaar van 2014 vertaald naar het domein van de ZBO's voor de verantwoordelijke bestuurders. Hierin zijn 11 sturingselementen of dashboardknoppen voor de rol van portefeuillehouder informatieveiligheid uitgewerkt.
- Voor de daadwerkelijke operationele mobilisatie zijn de door de IBD ontwikkelde BIG-OP producten vertaald naar het domein van de ZBO's: ruim 20 concrete handreikingen voor de invulling van de operationele maatregelen (Handreiking Mobile Devices, Logging-beleid, een format Beleidsplan, etc.) zijn ontwikkeld. Daarmee wordt een extra impuls gegeven aan de implementatie van de BIR, alsook dat de samenwerking op dit vlak vergemakkelijkt door uniforme maatregelen (verbetering van de interoperabiliteit binnen de overheidslaag als daarbuiten).

IV. Bereik ZBO

Voor de ZBO's is een bijdrage geleverd aan een aantal grote congressen door middel van presentaties en (teasers van) workshops. De nadruk heeft echter gelegen op het creëren van draagvlak voor de gekozen aanpak bij enerzijds relevante gremia als SIB, ICCIO en ICBR en anderzijds bij de departementen en de ZBO's zelf. Voor de ZBO's is per departement gekeken waar de behoeften van de onderhavige ZBO's lagen.

16 In Art. 41 lid 1 Kzbo is een algemene zorgplicht ten aanzien van informatiebeveiliging opgenomen:
"Een zelfstandig bestuursorgaan draagt op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorg voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens."
17 Klein Lef is een groep van kleine uitvoeringsorganisaties die diensten leveren aan burgers en bedrijven.



BIJLAGE

IV Provincies

IV Provincies

I. Organiseren verplichtende zelfregulering Provincies

De provincies hebben, ondersteund door de Taskforce BID, een convenant “Interprovinciale Regulering Informatieveiligheid” opgesteld, waarin vastgelegd is hoe zij invulling geven aan verplichtende zelfregulering. Dit convenant is op 13 november 2014 door het IPO-bestuur vastgesteld. Het bouwt daarmee ook voort op de de Interprovinciale Baseline Informatiebeveiliging (IBI) die de provincies hanteren sinds 2010.

Voor 2014 hebben de provincies een jaarplan opgesteld dat op hoofdlijn uitwerking geeft aan de onderdelen: bewustwording, leren, verantwoording, transparantie en de aansluiting op het Nationaal Respons Netwerk (NRN) van het NCSC. Daarnaast werken de provincies intern aan de versterking van informatieveiligheid binnen de eigen organisatie.

II. Gerichtheid Provincies

- De provincies hebben een programma opgesteld voor gezamenlijke activiteiten om te komen tot versterking van de gerichtheid op informatieveiligheid. Deze activiteiten richten zich met name op het bestuurders en op de ambtelijke top.
- Het aanbod is onder aandacht gebracht van de bestuurlijke adviescommissies van het interprovinciale overleg en via diverse communicatie kanalen richting alle relevante (vakgerelateerde) interprovinciale samenwerkingsverbanden.
- Voor de provincies is het campagnemateriaal voor bewustwording, dat in het kader van iBewustzijn Overheid is ontwikkeld, ook ontsloten en ingezet ten tijde van van Alert Online 2014 en daarna.

III. Verankering Provincies

Om verplichtende zelfregulering bij provincies te verankeren, is het noodzakelijk dit proces te integreren in de interne planning en control-cyclus van organisaties. In eerste instantie gaat het om de verdere implementatie van de Interprovinciale Baseline Informatiebeveiliging (IBI). De provincies hebben een standaardproces ontwikkeld dat erin voorziet dat op basis van een PDCA-cyclus een jaarlijks implementatieplan op te stellen, waarvan de uitvoering wordt gemonitord. De resultaten worden gebruikt om over de voortgang te rapporteren en dienen tevens als input voor het opstellen van het volgende jaarplan. De provincies zullen dit proces in het 4e kwartaal van 2014 ambtelijk vaststellen, om deze vervolgens te verbinden met de planning en control cyclus en zo de verankering te realiseren door het produceren van een in control statement.

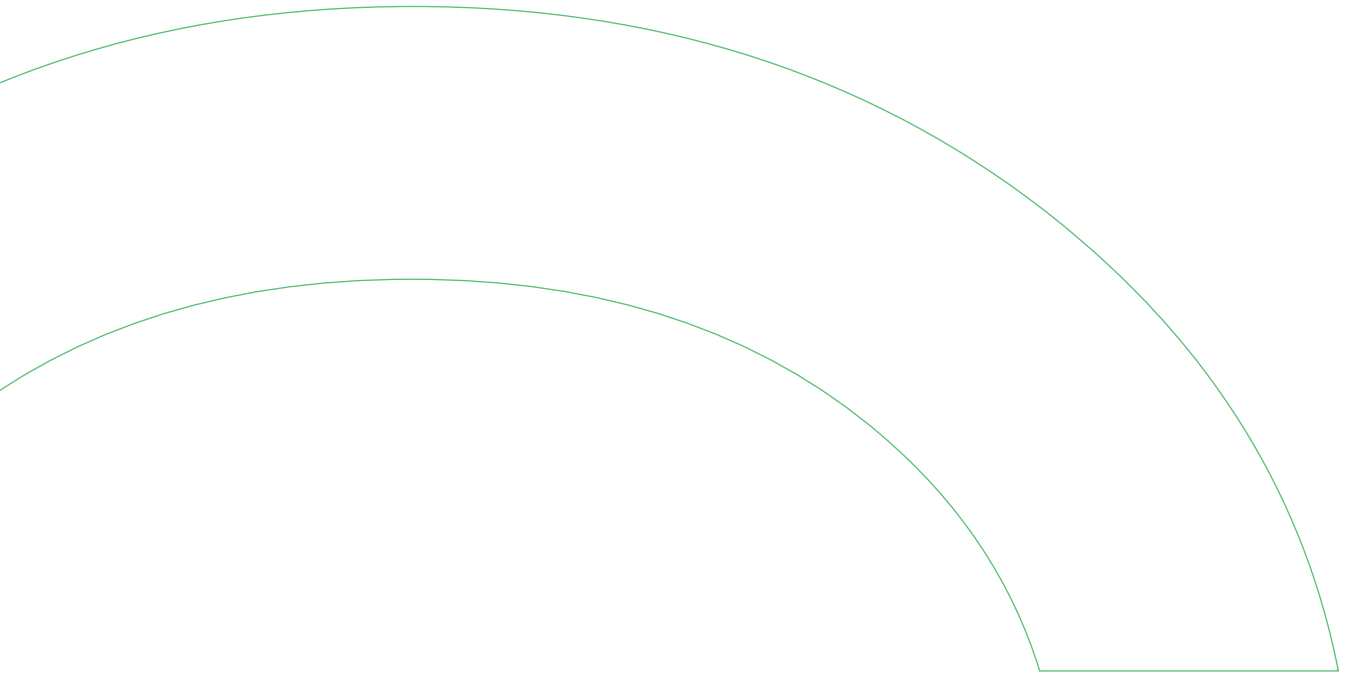
De interprovinciale vakgroep voor informatieveiligheid, CIBO (centraal informatiebeveiligers overleg), beheert reeds enkele producten, zoals de IBI, een tool voor business impact analyse en een monitoringtool voor verantwoording en transparantie. Het CIBO zal samen met de Taskforce vaststellen hoe borging en doorontwikkeling door provincies van deze producten verder ingericht kan worden.

Ten behoeve van de verankering van informatieveiligheid heeft de Taskforce naast het reguliere aanbod een aantal provincie-specifieke producten opgeleverd. Deze producten zijn fysiek verspreid tijdens eigen bijeenkomsten en bijeenkomsten van onze partners. Waar mogelijk zijn deze producten ook digitaal aangeboden via de website van de Taskforce BID, de deelsite informatieveiligheid op Pleio en via de websites van onze partners. Het gaat hierbij om:

- Specifieke factsheets /handreikingen voor doelgroepen binnen de provincies (bestuurders, provinciesecretarissen, gedeputeerden en (lijn)managers). Deze factsheets en handreikingen gaan in op de specifieke stuurvragen die vanuit de desbetreffende rol relevant zijn en het ondersteunde leeraanbod van de Taskforce BID. Deze handreikingen helpen bestuurders en managers om zich bewust te zijn van de risico’s en kwetsbaarheden, alsook om procesmatig de goede vragen kunnen stellen.
- De binnen het gemeentelijke domein ontwikkelde “Toolkit Informatieveiligheid Gemeentesecretarissen” is in het najaar van 2014 vertaald naar het provinciaal domein voor de provinciesecretarissen. Hierin zijn 11 sturingselementen of dashboardknoppen voor de rol van provinciesecretarissen/algemeen directeur uitgewerkt.
- Voor de daadwerkelijke operationele mobilisatie zijn de door de IBD ontwikkelde BIG-OP producten vertaald naar het domein van de provincies: IBI-OP. Hiermee krijgen provincies ruim 20 concrete handreikingen voor de invulling van de operationele maatregelen (Handreiking Mobile Devices, Logging-beleid, een format Beleidsplan, etc.). Daarmee wordt een extra impuls gegeven aan de implementatie van de IBI, alsook dat de samenwerking op dit vlak vergemakkelijkt door uniforme maatregelen (verbetering van de interoperabiliteit binnen de overheidslaag als daarbuiten).

I. Bereik Provincies

De inzet om de bewustwording bij provincies te vergroten richtte zich met name op bestuurders en de ambtelijke top. Daarnaast is er expliciet aandacht besteed aan de realisatie van verplichtende zelfregulering in een aantal werkconferenties en dialoogsessies. Zo heeft een dialoogsessie plaatsgevonden met de Kring van provinciesecretarissen en ook met de directeuren Middelen.



BIJLAGE

Waterschappen

V

V Waterschappen

I. Organiseren verplichtende zelfregulering Waterschappen

Om invulling te geven aan de gemaakte afspraken over verplichtende zelfregulering is op sectorniveau een stuurgroep informatieveiligheid gevormd onder leiding van de Unie van Waterschappen (UvW) en onder voorzitterschap van de secretaris directeur van een van de waterschappen. Deze stuurgroep heeft een programmaplan opgesteld met daarin de kaders, ambitie en governance voor verplichtende zelfregulering bij Waterschappen. Een belangrijke basis vormt een uniforme norm voor informatieveiligheid. Met ondersteuning van de Taskforce heeft de UvW daarom in de zomer van 2013 een gezamenlijke norm uitgewerkt, de Baseline informatieveiligheid Waterschappen (BIWA), welke is afgeleid van de BIG. De BIWA is samen met het programmaplan Informatieveiligheid Waterschappen bestuurlijk vastgesteld door UvW en bekrachtigd tijdens een speciaal daarvoor georganiseerd symposium informatieveiligheid begin oktober 2013. Meting op de voortgang van de implementatie van de BIWA en het programmaplan verloopt via waterschapsspiegel en waterschapspeil. Op sectorniveau zijn afspraken gemaakt en geborgd over de taken en verantwoordelijkheden van elk waterschap en van de UvW.

II. Gerichtheid Waterschappen

Via verschillende regionale sessies is ingezet op bewustwording en gerichtheid bij bestuurders en topmanagers op het thema informatieveiligheid. De Waterschappen hebben aangegeven in 2014 een bewustwordingscampagne uit te willen voeren, waarbij gebruik gemaakt zal worden van de generieke campagne iBewustzijn Overheid. Hiermee wordt aandacht gegeven aan houding en gedrag van medewerkers omtrent informatieveiligheid. Ten behoeve van bewustwording en vaardigheden omtrent incident- en crisisbeheersing loopt een pilot rond aansluiting bij het Nationaal Response Netwerk (NRN) waarin samenwerking tussen waterschappen wordt gestimuleerd. Voor alle waterschappen is in het najaar een internationale training georganiseerd bij het ENCS (European Network for Cyber Security) gericht op informatieveiligheid en ICS/SCADA (industriële controle systemen). Aansluitend op deze training heeft de Taskforce BID een middagprogramma georganiseerd voor hoofden en coördinatoren I&A om hen bewust te maken van de risico's die hier specifiek aan verbonden zijn.

III. Verankering Waterschappen

Om de voortgang in de uitvoering van de programmering rondom informatieveiligheid te bespreken, de onderlinge kennisuitwisseling te stimuleren en elkaar te informeren over actuele zaken, is er een landelijk overleg voor de contactpersonen informatiebeveiliging georganiseerd vanuit UvW en HWH. Via diezelfde programmering werken Waterschappen aan verankering op de volgende vlakken:

- Het opstellen en vaststellen van een beleidsplan informatieveiligheid met doelen, maatregelen en budget;
- Het in de begroting opnemen van het benodigde budget om informatieveiligheid adequaat in te kunnen richten;
- De implementatie van de BIWA;
- Het inrichten van een PDCA-cyclus informatieveiligheid als onderdeel van de reguliere P&C-cyclus;
- Het meten van informatieveiligheid aan de hand van indicatoren
- Het aanleveren van de meting naar de koepel (UvW) t.b.v. een beeld over de overheidslaag heen;
- Het treffen van voorbereidingen voor een audit op informatieveiligheid;
- Het inrichten van incidentregistratie en incidentrapportages.

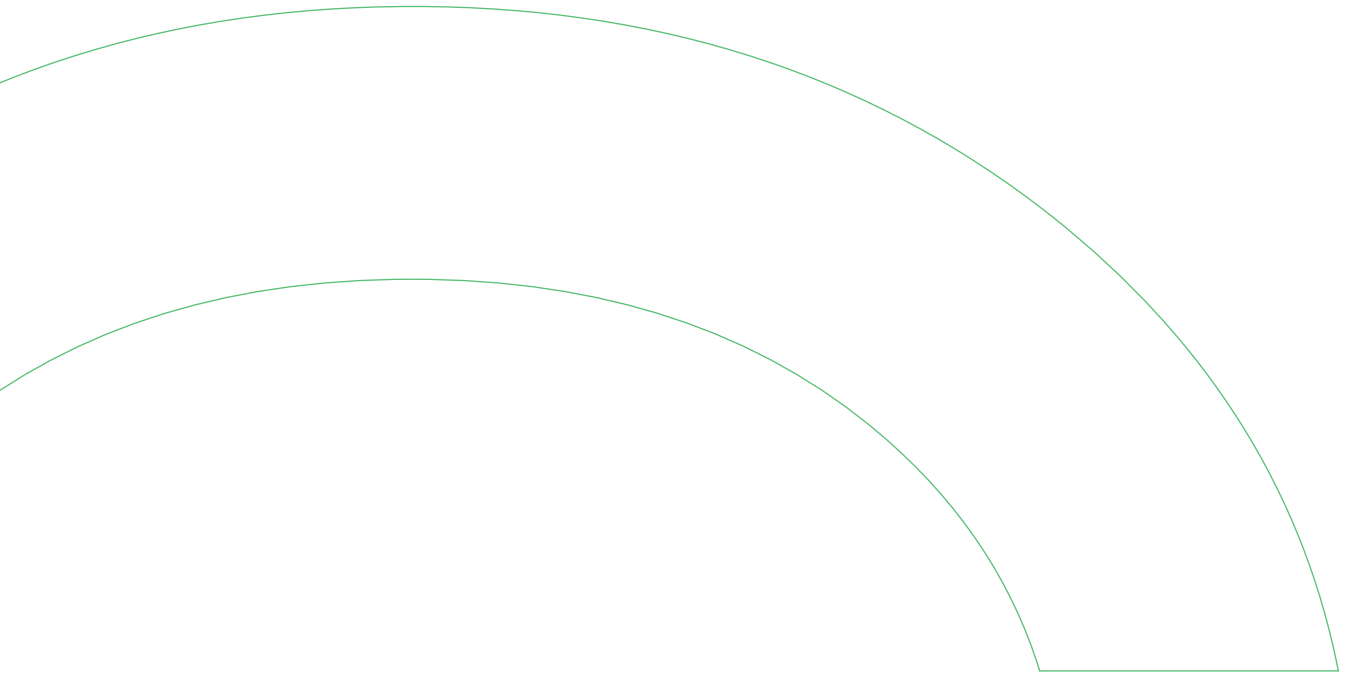
Ten behoeve van de verankering van informatieveiligheid heeft de Taskforce, naast het reguliere aanbod, een aantal waterschapspecifieke producten opgesteld. , die o.A. ontsloten worden via de website van de Taskforce BID, de deelsite informatieveiligheid op Pleio en via de websites van partners. Het gaat hierbij om:

- Specifieke factsheets /handreikingen voor doelgroepen binnen de waterschappen (dijkgraven, secretaris-directeuren, bestuursleden en lijnmanagers). Deze factsheets en handreikingen gaan in op de specifieke stuurvragen die vanuit de desbetreffende rol relevant zijn en het ondersteunde leeraanbod van de Taskforce BID. Deze handreikingen helpen bestuurders en managers om zich bewust te zijn van de risico's en kwetsbaarheden, alsook om procesmatig de goede vragen kunnen stellen.
- De binnen het gemeentelijke domein ontwikkelde "Toolkit Informatieveiligheid Gemeentesecretarissen" is in het najaar van 2014 vertaald naar het domein van de waterschappen voor de secretaris-directeuren. Hierin zijn 11 sturingselementen of dashboardknoppen voor de rol van secretaris-directeur/algemeen directeur uitgewerkt.

- Voor de daadwerkelijke operationele mobilisatie zijn de door de IBD ontwikkelde BIG-OP producten vertaald naar het domein van de waterschappen: BIWA-OP. Hiermee krijgen waterschappen ruim 20 concrete handreikingen voor de invulling van de operationele maatregelen (Handreiking Mobile Devices, Logging-beleid, een format Beleidsplan, etc.). Daarmee wordt een extra impuls gegeven aan de implementatie van de BIWA, alsook dat de samenwerking op dit vlak vergemakkelijkt door uniforme maatregelen (verbetering van de interoperabiliteit binnen de overheidslaag als daarbuiten).

IV. Bereik Waterschappen

Om bewustzijn omtrent informatieveiligheid te vergroten zijn in 2013 diverse toelichtingen gegeven bij landelijke overleggen van secretaris-directeuren, verantwoordelijk (lijn)management en de betrokken IB-functionarissen als ook betrokken vakgroepen. Daarnaast zijn aparte evenementen ingezet om specifieke doelgroepen te bereiken. Tijdens het landelijk symposium informatieveiligheid begin oktober 2013 zijn bestuurders en directies van waterschappen geïnformeerd over informatieveiligheid en de gemaakte afspraken over de invulling van verplichtende zelfregulering bij waterschappen. Het jaarlijkse tweedaagse congres van de KRIHCIA (Kring van Hoofden Informatievoorziening & Automatisering) eind 2013 heeft volledig in het teken gestaan van informatieveiligheid. In het najaar van 2014 zijn twee regionale bijeenkomsten voor Waterschapsbestuurders georganiseerd en een interbestuurlijke masterclass voor bestuurders van mede-overheden in Noord Nederland.



BIJLAGE

Gemeenten VI

VI Gemeenten

I. Organiseren verplichtende zelfregulering Gemeenten

Om het thema informatieveiligheid op de agenda te krijgen in het gemeentelijke domein heeft de Taskforce BID de Vereniging Nederlandse Gemeenten (VNG) ondersteund bij het opstellen van de Resolutie 'Informatieveiligheid, randvoorwaarde voor een professionele gemeente'. Deze Resolutie is eind 2013 aangenomen door 94,8% van de aanwezige gemeenten tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de VNG. Hiermee is vorm gegeven aan de invulling van verplichtende zelfregulering. De Resolutie gaat in op de verantwoordelijkheid van iedere afzonderlijke gemeente om een informatieveiligheidsbeleid vast te stellen aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die is opgesteld door de IBD. Tevens zullen gemeenten informatieveiligheid zowel bestuurlijk als ambtelijk borgen en maken ze de invulling op informatieveiligheid transparant voor burgers, bedrijven en ketenpartners.

Er is onderzoek verricht naar de verschillende samenwerkingsvormen binnen het gemeentelijk domein, in het bijzonder waar het gaat om verlengd lokaal bestuur, en welke extra vraagstukken dit geeft ten aanzien van informatieveiligheid. Daarnaast is in samenwerking met LOCGS een position paper geschreven op dit thema en is met het veiligheidsberaad gewerkt aan een plan van aanpak voor de inbedding van informatieveiligheid in de veiligheidsregio's.

II. Gerichtheid Gemeenten

In het verlengde van de Resolutie zijn met andere gemeentelijke vakverenigingen convenanten gesloten om de uitvoering van de Resolutie verder te verankeren en de basis te leggen voor een brede uitrol van de Resolutie in het gemeentelijke domein. De belangrijkste doelgroepen daarbij zijn de raadsleden, burgemeesters en wethouders, gemeentesecretarissen en lijnmanagers. Om deze groepen te bereiken zijn er convenanten gesloten met:

- Vereniging Directeuren Publieksdiensten (VDP)
- Raadslid.nu
- Vereniging van Gemeentesecretarissen (VGS)
- Nederlandse Vereniging voor Burgerzaken (NVVB)

Daarnaast is er met een aantal andere gemeentelijke vakverenigingen productieve werkafspraken gemaakt, onder andere met het Nederlands Genootschap van Burgemeesters (NGB), de Provinciale Afdelingen van de VNG, de FAMO (Federatie van Algemene Middelenmanagers bij de Overheid) en de VIAG (Vereniging van Coördinatoren I&A van Gemeenten).

De genoemde doelgroepen zijn enerzijds bereikt via bijdragen aan de al bestaande regionale en landelijke congressen, anderzijds heeft de Taskforce in samenwerking met bovenstaande partijen specifieke bijeenkomsten belegd. Bijvoorbeeld door het organiseren van "learn and share" sessies voor burgemeesters en wethouders voor alle provinciale afdelingen van de VNG en workshops voor de regionale kringen van gemeentesecretarissen van de VGS.

Daarnaast heeft de Taskforce heeft op uiteenlopende wijze, samen met VNG en IBD, gemeenten in staat gesteld en gestimuleerd om met de elementen van de Resolutie aan de slag te gaan:

- Voor 20 gemeenten van Dimpact en GovUnited[18] is in samenwerking met de IBD een leercommunity informatieveiligheid voor CISO's opgezet. In totaal zijn er vijf bijeenkomsten georganiseerd. In oktober 2014 vindt een slotconferentie plaats voor alle 50 gemeenten die zijn aangesloten bij Dimpact en GovUnited
- De Taskforce heeft bijgedragen geleverd aan workshops en ronde tafelgesprekken over het thema informatieveiligheid. Veelal met betrekking tot de decentralisaties. Zo zijn er gerichte bijdragen geleverd aan het Living Lab Oost- Nederland, Ronde tafel conferentie Decentralisaties en de Raad op Zaterdag.
- In het kader van een afstudeeropdracht is de voortgang van de implementatie van de Resolutie Informatieveiligheid onderzocht bij alle 56 Gelderse gemeenten.
- Met Raadslid.nu is een enquête onder alle 1600 raadsleden uitgezet over het belang van informatieveiligheid, waarvan de uitkomsten eind 2014 gepresenteerd zullen worden tijdens het najaarscongres van raadslid.nu.
- Met de rekenkamer Den Haag en de Nederlandse Vereniging van Rekenkamer is een workshop verzorgt op de Algemene Leden Vergadering, daarnaast is een handreiking rekenkameronderzoek informatieveiligheid opgesteld en verzonden aan alle rekenkamers.

III. Verankering Gemeenten

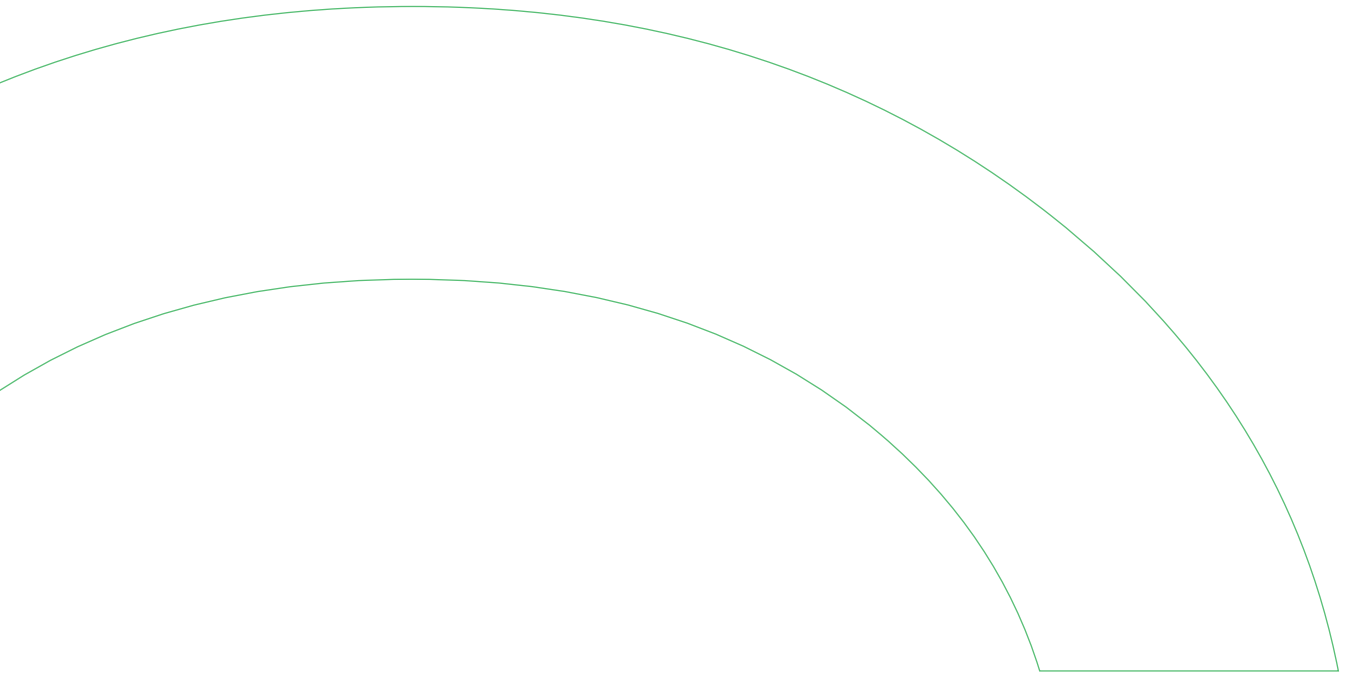
Ten behoeve van de verankering van informatieveiligheid heeft de Taskforce naast het reguliere aanbod een aantal gemeentespecifieke producten opgeleverd. Deze producten zijn fysiek verspreid tijdens eigen bijeenkomsten en bijeenkomsten van onze partners. Waar mogelijk zijn deze producten ook digitaal aangeboden via de website van de Taskforce BID, de deelsite informatieveiligheid op Pleio en via de websites van onze partners. Het gaat hierbij om:

- Specifieke factsheets /handreikingen voor gemeentelijke doelgroepen (bestuurders, gemeentesecretarissen, raadsleden en lijnmanagers). Deze factsheets en handreikingen gaan in op de specifieke stuurvragen die vanuit de desbetreffende rol relevant zijn en het ondersteunde leeraanbod van de Taskforce BID. Deze handreikingen helpen bestuurders en managers om zich bewust te zijn van de risico's en kwetsbaarheden, alsook om procesmatig de goede vragen kunnen stellen.
- In samenwerking met de VGS en de VNG is een "Toolkit Informatieveiligheid Gemeentesecretarissen" ontwikkeld specifiek voor gemeentesecretarissen. Hierin zijn 11 sturingselementen of dashboardknoppen voor de rol van gemeentesecretaris/ algemeen directeur uitgewerkt. Deze toolkit wordt op dit moment vertaald naar een generiek document voor de andere overheidslagen.
- Voor de daadwerkelijke operationele mobilisatie is ondersteuning verleend aan de IBD voor de ontwikkeling van de zogeheten BIG-OP producten. Hiermee biedt IBD aan gemeenten concrete handreikingen voor de invulling van de operationele maatregelen. Hiermee wordt een impuls gegeven aan de implementatie van de BIG, alsook dat de samenwerking op dit vlak vergemakkelijkt door uniforme maatregelen (verbetering van de interoperabiliteit binnen de overheidslaag als daarbuiten).

IV. Bereik Gemeenten

In het kader van de samenwerking met de NGB, VNG, VGS en de provinciale afdelingen van de VNG zijn een achttal 'learn and share' bijeenkomsten georganiseerd voor burgemeesters, wethouders en gemeentesecretarissen. In opvolging van de samenwerking met de VGS is aan alle kringen van gemeentesecretarissen het aanbod gedaan voor het organiseren van een workshop informatieveiligheid. Circa 2/3 van de actieve kringen is op dit aanbod ingegaan (in totaal 10). Daarnaast heeft de Taskforce acte presence gegeven bij een aanzienlijk aantal (grote) congressen, zoals het KING jaarcongres, VNG Jaarcongres, het VGS jaarcongres 2013 en de regiocongressen van de NVVB en Raadslid.nu. Tijdens deze congressen en andere symposia zijn ook een aantal workshops en hack demonstraties verzorgd.

18 Dimpact en Govunited zijn twee gemeentelijke inkoopcombinatie waarin gemeenten gezamenlijk een van de belangrijkste onderdelen van de gemeentelijke ICT voorzieningen hebben aanbesteed. Het betreft zogeheten 'zaaksystemen' waarmee gemeenten de afhandeling van hun (elektronische) dienstverlening vormgeven.



BIJLAGE

Rapport Onderzoeksraad voor Veiligheid - Aanbevelingen DigiNotar

VII

VII Rapport Onderzoeksraad voor Veiligheid - Aanbevelingen DigiNotar

De Onderzoeksraad richt zijn aanbevelingen op overheidsorganisaties. De reden hiervoor is dat overheidsorganisaties zelf verantwoordelijk zijn voor het veilig beheer van de gegevens die zij onder zich hebben. Als zij ervoor kiezen externe partijen hierbij te betrekken moeten zij zich er als goed opdrachtgever van vergewissen dat deze partij aan de door hen gestelde eisen en doelen voldoet[19].

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

1. Zorg dat bestuurders van alle overheidsorganisaties hun verantwoordelijkheid nemen voor het beheersen van digitale veiligheid.

Daartoe moet u een programma ontwikkelen dat bestuurders van overheidsorganisaties doordringt van het belang van digitale veiligheid, en hen voorziet van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie.

Ook moet u overheidsorganisaties verplichten om zich te verantwoorden over de wijze waarop zij digitale veiligheid waarborgen. Veranker daartoe een duidelijk omschreven openbare verantwoordingsplicht op het gebied van digitale veiligheid in de planning & controlcyclus van overheidsorganisaties, en laat bestuurders van overheidsorganisaties jaarlijks een 'in control statement' voor digitale veiligheid afgeven.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Veiligheid en Justitie

2. Schep voorwaarden zodat overheidsorganisaties hun digitale veiligheid systematisch beheersen

Hiertoe moet u ervoor zorgen dat alle overheidsorganisaties de open standaarden NEN-ISO/IEC 27001 en 27002 naleven, die gezamenlijk een kader voor systematische digitale veiligheidszorg bieden. Stel daarvoor een plan op waarin concrete doelen, maatregelen en een tijdspad worden benoemd. Wijs bovendien een organisatie aan die overheidsorganisaties kan begeleiden bij het tot stand brengen van adequate digitale veiligheidszorg.

Als onderdeel van een dergelijke systematische aanpak moet vanuit gemeenten, veiligheidsregio's en de rijksoverheid aandacht bestaan voor het voorbereid zijn op, en het herstellen van schade als gevolg van, digitale incidenten. Burgers en bedrijven wier gegevens door een digitaal veiligheidsincident zijn getroffen, moeten kunnen volstaan met dit één keer te melden waarna adequate maatregelen moeten worden getroffen door alle betrokken overheidsorganisaties.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Economische Zaken

3. Realiseer een veiliger uitgifte en gebruik van digitale certificaten

Pas hiervoor de rol van OPTA en Logius zodanig aan, dat sprake is van werkelijk toezicht op en handhaving van de feitelijke naleving door certificaatdienstverleners van de vigerende regelgeving ten aanzien van gekwalificeerde en PKIoverheid-certificaten.

Bevorder daarnaast een cultuuromslag bij alle partijen die bij certificaatdienstverlening betrokken zijn, in het bijzonder ten aanzien van het melden en leren van incidenten. Maak daarbij gebruik van ervaringen met veilig melden uit andere sectoren.

19 www.onderzoeksraad.nl/uploads/items-docs/1094/Rapport_Diginotar_NL_web_def_20062012.pdf

BIJLAGE

VIII Afkortingen

VIII Afkortingen

ARM	Advanced Risk Management
BALV	Buitengewone Algemene Ledenvergadering
BID	Bestuur en Informatieveiligheid Dienstverlening
BIG	Baseline Informatiebeveiliging Gemeenten
BIR	Baseline Informatiebeveiliging Rijksdienst
BIWA	Baseline Informatiebeveiliging Waterschappen
BZK	Ministerie van Binnenlandse zaken en Koninkrijksrelaties
CIBO	Centraal Informatie Beveiligings Overleg
CIP	Centrum Informatiebeveiliging en privacybescherming
CISO	Chief Information Security Officer
DGOBR	Directoraat- Generaal Organisatie Bedrijfsvoering Rijk
ENCS	European Network for Cyber Security
ENSIA	Eenduidige Normatiek, Single Information en Audit
EZ	Ministeries van Economische Zaken
FAMO	Federatie van Algemene Middelenmanagers bij de Overheid
HSD	The Haque Security Delta
HWH	Het Waterschapshuis
IBD	Informatie Beveiligings Dienst
IBI	Interprovinciale Baseline Informatiebeveiliging
ICBR	Interdepartementale Commissie Bedrijfsvoering Rijksdienst
ICCIO	Interdepartementale Commissie Chief Information officers
ICS	Industrial Control Systems

IPO	Inter Provinciaal overleg
IRAM	Information Risk Analysis Methodology
ISO	Internationale organisatie voor standardisatie
KRIHCIA	Kring van Hoofden Informatievoorziening & Automatisering
MAPGOOD	Mensen, Apparatuur,Programmatuur, Gegevens, Organisatie, Omgeving, Diensten
NCDO	Nationaal Commissaris Digitale Overheid
NCSC	Nationaal Cyber Security Centrum
NEN	Nederlandse Norm
NGB	Nederlandse Genootschap van Burgemeesters
NRN	Nationaal Respons Netwerk
NVVB	Nederlandse vereniging voor Burgerzaken
RBB	Rijksbrede Benchmark groep
SCADA	Supervisory Control And Data Acquisition
SIB	Subcommissie Informatie Beveiliging en Privacy
TTISC	Towards Trustworthy ICT Service Chains
UvW	Unie van Waterschappen
VDP	Vereniging Directeuren Publieksdiensten
VGS	Vereiniging van Gemeentensecretarissen
VIAG	Vereiniging van coördinatoren I&A van Gemeenten
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VNG	Vereniging Nederlandse Gemeenten
ZBO	Zelfstandig Bestuursorgaan