Nationaal detectie netwerk

Plan van aanpak pilot netwerkdetectie Rijksinternetvoorziening

Projectgroep

28-11-2013

Projectgroep	
Betrokken organisaties	De pilot netwerkdetectie Rijksinternetvoorziening wordt uitgevoerd in een samenwerkingsverband van BZK (DG OBR), BZK (AIVD), BZK (SSC-ICT), DEF (MIVD), V&J (NCSC).
(Beoogd) opdrachtgever	BZK/DG OBR
(Beoogde) opdrachtnemers	V&J/DCS/NCSC, BZK/AIVD, DEF/MIVD, BZK/SSC-ICT
Contactpersonen	[redacted]

Wijzigingenbeheer

Datum	*Versie*	*Wijzigingen*	*Gewijzigd door*
26.07.2013	0.9.1	Aangepaste opzet document, deels nieuwe en gewijzigde tekstdelen	[redacted]
05.08.2013	0.9.2	Verwerking commentaar n.a.v. overleg op 30 juli en bijdragen van [redacted] voor governance, kosten en resultaten	[redacted]
08.08.2013	0.9.3	Verwerking commentaar nav schriftelijke ronde 5 augustus 2013.	[redacted]
15.08.2013	0.9.4	Verwerking opmerkingen [redacted] nav voorbereiden verzenden stukken naar MT OBR	[redacted]
20.08.2013	0.9.5	Toevoeging Defensie-industrie in inleidende hoofdstukken (waar het NDN betreft, niet specifiek de pilot), voetnoot met verklaring defensie-industrie en aanvullende tekst in paragraaf 2.2.1.	[redacted]
22.08.2013	0.9.6	Toevoegen opmerkingen [redacted]	[redacted]
30.08.2013	0.9.9	Wijzigingen in paragraaf 3.4 over medezeggenschap nav advies SZW en besluit MT OBR	[redacted]
20.09.2013	0.9.95	Wijziging in paragraaf 3.4 nav PIA	[redacted]
15.11.2013	0.9.96	Actualisering alle paragrafen	[redacted]
21.11.2013	0.9.98	Verwerken opmerkingen [redacted], doorvoeren wijzigingen en verbeteren terminologie.	[redacted]
22.11.2013	1.0		

Inhoudsopgave

Inhoud

Managementsamenvatting 5

1. Inleiding 7
   1.1 Achtergrond pilot netwerkdetectie Rijksinternet 7
   1.2 Doel en werking van het nationaal detectie netwerk 7
   1.3 Locatie van de pilot 8

2. Pilot netwerkdetectie Rijksinternet 10
   2.1 Doelstelling van de pilot 10
   2.2 Opzet van de pilot 10
   2.2.1 Procesbeschrijving tijdens de pilot 10
   2.2.2 Technische opstelling tijdens de pilot 11
   2.3 Verwachte resultaten 12
   2.4 Bereik 13
   2.5 In werking treden detectie 13
   2.6 Operationele randvoorwaarden van de pilot 14

3. Medezeggenschap en privacy 15
   3.1 Taken, verantwoordelijkheden en waarborgen AIVD 15
   3.2 Taken, verantwoordelijkheden en waarborgen NCSC 15
   3.3 Verwerking persoonsgegevens 16
   3.4 Betrokkenheid medezeggenschap in relatie tot de pilot 17
   3.5 Waarborgen zorgvuldige omgang met gegevens 18

4. Organisatie van de pilot 19
   4.1 Governance pilot 19
   4.2 Melden van detectie aan pilot departementen 20
   4.3 Besluitvorming over de pilot 21
   4.4 Investeringsanalyse 21
   4.5 Communicatie over de pilot 22

5. Planning 23
   5.1 Randvoorwaarden 23
   5.2 Mijlpalenplanning 23

6. Beheersing 24
   6.1 Go/No-go 24
   6.2 Voortgangsrapportage 24
   6.3 Kwaliteitsborging 24
   6.4 Oplevering en vervolg 25

7. Projectrisico's 26

Verklarende woordenlijst 27

Bijlagen 28

Managementsamenvatting

1. Aanleiding

Minister Opstelten van Veiligheid en Justitie heeft aan de Tweede Kamer de toezegging gedaan om in 2014 een nationaal detectie netwerk (NDN) op- en uit te bouwen. Het doel van het NDN is te komen tot een netwerk van samenwerkende publieke organisaties en private organisaties uit de kritieke infrastructuur die, ondersteund en gefaciliteerd door de Algemene Inlichtingen en Veiligheidsdienst (AIVD), Militaire Inlichtingen en Veiligheidsdienst (MIVD) en het Nationaal Cybersecurity Center (NCSC), detectieactiviteiten uitvoeren naar digitale dreigingen op basis van hoogwaardige dreigings- en incidenteninformatie die binnen dit netwerk wordt uitgewisseld. Deze detectie verhoogt de weerbaarheid tegen digitale aanvallen, omdat organisaties informatie met elkaar kunnen uitwisselen over digitale dreigingen. Aanleiding voor het NDN is de toenemende mate waarin Nederland het doelwit is van digitale aanvallen.

Om het NDN te kunnen realiseren, heeft het ministerie van Veiligheid en Justitie DGOBR verzocht opdrachtgever te zijn voor een pilot op de Rijksinternetvoorziening. Op de Rijksinternetvoorziening bestaat geschikt netwerkverkeer met voldoende volume. Meerdere rijksoverheidsorganisaties zijn betrokken vanwege hun aansluiting op het Rijksinternet en SSC-ICT is aanwezig als professionele beheerorganisatie die tevens ruime ervaring heeft met netwerkdetectie.

2. Doelstelling

De doelstelling van de pilot is te onderzoeken en vast te stellen of de specifieke dienstverlening van de AIVD en het NCSC, daadwerkelijk bijdraagt aan het tijdig ontdekken van belangrijke digitale dreigingen gericht op die Rijksoverheid. Tijdens de pilot wordt informatie over dreigingen uitgewisseld zodat beter zicht wordt verkregen op het aantal, het type aanvallen en de opvolging ervan. De duur van de pilot bedraagt zes maanden.

3. Randvoorwaarden

De pilot kent een aantal belangrijke randvoorwaarden. De belangrijkste daarvan zijn 1) het borgen van betrokkenheid van de medezeggenschap en 2) het borgen van een zorgvuldige omgang met persoonsgegevens.

Medezeggenschap: Gedurende de voorbereiding van de pilot, is tijdens overleg tussen BZK, V&J en SZW geconstateerd dat de pilot een brede casus aanhangig maakt. Doordat ICT-voorzieningen veelal bij SSC-ICT zijn ondergebracht, ontstaat een nieuwe situatie indien wijzigingen optreden ten aanzien van (het gebruik van) beveiligingssoftware en bestaat er een behoefte aan het harmoniseren van de Internet- en gedragscodes. In de Internet- en gedragscode wordt beschreven op welke wijze medewerkers horen om te gaan met het gebruik van e-mail en Internet. In een dergelijke code wordt vaak melding gemaakt van de persoonsgegevens die worden gelogd om toezicht te kunnen houden op een veilig gebruik van Internet en e-mail. Gezien het rijksbrede karakter van een geharmoniseerde Internet- en gedragscode, is het Overleg Orgaan Rijk (OOR) het meest aangewezen gremium om de medezeggenschap hierover te organiseren.

De pilot detectie Rijksinternetvoorziening wordt gebruikt als input voor het traject waarin de OOR om instemming wordt gevraagd voor een nieuwe geharmoniseerde gedrags- en internetcodes. De input die de pilot oplevert met betrekking tot dit punt, is ook één van de resultaten van de pilot. Het proces rond het harmoniseren van Internet- en gedragscodes behoort niet tot de scope van de pilot, omdat dit een bredere casus betreft.

Verwerking persoonsgegevens

In de monitoring van netwerkverkeer en de bijbehorende detectie, komen persoonsgegevens voor. IP-adressen en e-mailadressen zijn hier een voorbeeld van. Het verwerken van persoonsgegevens dient zorgvuldig te gebeuren. Daarom is voorafgaand aan de pilot het Rijksplatform van Privacyfunctionarissen (RPPF) geraadpleegd. De RPPF heeft geadviseerd een Privacy Impact Assessment (PIA) uit te voeren. Deze PIA is uitgevoerd in samenwerking met de functionarissen gegegevensbescherming van de ministeries BZK en Veiligheid en Justitie. Het resultaat van de PIA wordt besproken met de RPPF. Een belangrijk onderdeel van het werken met persoonsgegevens is de bewaartermijn en de vernietiging van de persoonsgegevens. Deze bewaartermijn is voor de pilot gesteld op 30 dagen. Op de vernietiging van de persoonsgegevens wordt toegezien door de Audit Dienst Rijk (ADR) voor het NCSC, voor de AIVD wordt dit gedaan door de Commissie van Toezicht betreffende de Inlichtingen- en VeiligheidsDiensten (CTIVD).

4. Werkwijze pilot

Twee sensoren worden geplaatst in de omgeving van de Rijksinternetvoorziening. [redacted] en is gericht op aanvallen op de digitale werkplekken bij de ministeries. Hiermee kunnen digitale aanvallen beter worden herkend. Wanneer een vreemd signaal wordt gedetecteerd, dan wordt dit gesignaleerd door SSC-ICT en doorgegeven aan AIVD of NCSC, afhankelijk van de sensor die het signaal detecteerde. Afhankelijk van het signaal worden vervolgacties opgepakt. Dit gebeurt in afstemming met SSC-ICT.

5. Resultaten

De pilot moet leiden tot de volgende deelresultaten:

1) Een nulmeting.

2) *Een maandelijkse rapportage aan SSC-ICT van de AIVD en het NCSC.*

3) *Een beproefde infrastructuur met bijbehorende processen en organisatie.*

4) *Een tussen- en een eindevaluatie.*

5) *Voortgangsrapportage privacy en medezeggenschap en input om het proces van medezeggenschap te organiseren met betrekking tot het harmoniseren van Internet- en gedragscodes.*

6) *Een beknopte incidentrapportage of incidentrapportages.*

7) *Een eindrapportage met een conclusie op basis van de resultaten.*

1. Inleiding

1.1 Achtergrond pilot netwerkdetectie Rijksinternet

Nederland is één van de meest gedigitaliseerde landen ter wereld. Digitalisering levert grote voordelen op en is een drijvende kracht achter onze welvaart. De keerzijde van digitalisering is echter dat wij ook kwetsbaar worden voor cyberdreigingen. Uit onderzoek van onder meer het NCSC, AIVD en MIVD blijkt dat de dreiging die uitgaat van digitale aanvallen blijft toenemen. Grote incidenten zoals Diginotar, de KPN-hack, Dorifel, de DDoS aanvallen en de aanhoudende gevallen van cyberspionage illustreren deze trend. Zij laten bovendien zien dat de complexiteit van deze aanvallen toeneemt en dat de potentiële maatschappelijke en economische impact groot kan zijn. De weerbaarheid van Nederland tegen deze dreigingen heeft geen gelijke tred gehouden met de digitalisering. Maatregelen worden versnipperd genomen en zijn veelal beperkt. Naar aanleiding van deze ontwikkelingen heeft de minister van Veiligheid en Justitie aan de Tweede Kamer toegezegd in 2014 een Nationaal Detectie Netwerk (NDN) te starten en vervolgens uit te bouwen dat digitale dreigingen kan onderkennen zodat hier tegen kan worden opgetreden. Met het NDN zal de digitale weerbaarheid van Nederland worden versterkt. Het NCSC is initiatiefnemer voor het NDN.

De AIVD, MIVD en het NCSC zullen samenwerken aan de realisatie van het NDN, gezien de expertise, ervaring en internationale relaties van deze organisaties. De drie organisaties vervullen daarnaast vaak initiërende en coördinerende taken en hebben ervaring met publieke en private samenwerking.

1.2 Doel en werking van het nationaal detectie netwerk

Het doel van het NDN is te komen tot een netwerk van samenwerkende publieke organisaties en private organisaties uit de kritieke infrastructuur die, ondersteund en gefaciliteerd door de AIVD, MIVD en het NCSC, detectieactiviteiten uitvoeren naar digitale dreigingen op basis van hoogwaardige dreigings- en incidenteninformatie die binnen dit netwerk wordt uitgewisseld.

Het NDN moet sneller en betere informatie uit kunnen wisselen over dreigingen en incidenten dan momenteel gebeurt. Wanneer kwaadwillenden digitale aanvallen voorbereiden en uitvoeren, blijft dat vaak niet onopgemerkt. In het internationale netwerk van inlichtingen- en veiligheidsdiensten en CERTs is informatie beschikbaar over die aanvallen. Door deze informatie middels indicatoren zo snel als mogelijk te delen met de organisaties uit de kritieke infrastructuur kunnen deze organisaties vaststellen of zij geraakt zijn door een digitale aanval en passende herstelmaatregelen nemen. Door vervolgens ook incidenteninformatie te delen, kan de aard en het bereik van een aanval worden vastgesteld. Op basis hiervan kan een organisatie overstijgend dreigingsbeeld worden opgesteld. De dreigingsinformatie die gedeeld wordt binnen het NDN kan betrekking hebben op dreigingen die een potentieel maatschappij ontwrichtende werking hebben of op een bedreiging voor de nationale veiligheid. Het NDN

richt zich daarmee niet op alle virussen op alle netwerken van alle Nederlandse organisaties, maar uitsluitend op rijksoverheid, vitale sectoren en de defensie-industrie[1].

De dreigings- en incidenteninformatie waarmee het netwerk wordt gevoed wordt deels door het netwerk zelf gegenereerd en deels, met name waar het gaat om de hoogwaardige dreigings- en incidentinformatie, door de AIVD, MIVD en het NCSC. Deze laatste drie organisaties hebben toegang tot bronnen die informatie bevatten die voor anderen niet of beperkt beschikbaar zijn. Ook beschikken zij over specifieke kennis en expertise, wat hen in staat stelt om partijen als de Rijksoverheid en de organisaties uit de vitale sectoren en defensie-industrie te ondersteunen. De AIVD, MIVD en het NCSC geven via het NDN invulling aan hun veiligheidsbevorderende taken ten aanzien van de nationale veiligheid en het voorkomen van maatschappelijke ontwrichting in Nederland.

Om het NDN te kunnen realiseren, is in 2013 een pilot bij de Rijksoverheid beoogd. De pilot is een voorloper van het NDN. De pilot draagt bij aan het doel van het NDN doordat inzicht wordt verkregen in technische, organisatorische en politiek- bestuurlijke aspecten die van belang zijn voor het realiseren van het uiteindelijke NDN. Omdat het NDN op langere termijn ook wordt toegepast in de vitale sectoren, wordt in 2013 ook gestart met een ronde tafel voor private organisaties. Doel van deze ronde tafel is voor te sorteren op de samenwerking die nodig zal zijn om het NDN verder uit te bouwen naar de vitale sectoren. De ervaringen die worden opgedaan in de pilot bij de rijksoverheid, worden gebruikt om het NDN verder op- en uit te bouwen, ook voor de vitale sectoren en de defensie-industrie. De pilot draagt bij aan een groter bewustzijn bij en een betere bescherming van de betrokken organisaties omdat indicaties van misbruik worden ontdekt en hierop door die organisaties tegenmaatregelen ondernomen kunnen worden.

1.3 Locatie van de pilot

Voor de pilot is gezocht naar een geschikte locatie. Die locatie is gevonden in de omgeving van het Rijksinternet[2]. Hier bestaat geschikt netwerkverkeer met voldoende volume. Meerdere rijksoverheidsorganisaties zijn betrokken vanwege hun aansluiting op het Rijksinternet en SSC-ICT is aanwezig als professionele beheerorganisatie die tevens ruime ervaring heeft met netwerkdetectie. De dienst die met het NDN wordt geïntroduceerd is voor SSC-ICT een aanvulling op haar bestaande dienstverlening. Omdat de pilot wordt gedaan nabij de Rijksinternetvoorziening wordt dit ook de naam van de pilot: "pilot netwerkdetectie Rijksinternetvoorziening".

1.4 Leeswijzer

In de beschrijving van het plan van aanpak wordt ingegaan op de volgende onderwerpen. In hoofdstuk twee wordt de doelstelling van de pilot beschreven, evenals de aanpak, het bereik en de verwachte resultaten van de pilot. Ook worden de verschillende technische aspecten

[1] *Alle* bedrijven die diensten of producten leveren aan Defensie en daarvoor moeten beschikken over gerubriceerde gegevens vallen onder ABDO regelgeving. De "defensie-industrie" is het overkoepelende begrip dat het geheel van bedrijven omvat waarvoor ABDO autorisatie is afgegeven door MIVD.

[2] Het Rijksinternet is een term die is afgesproken met SSC-ICT en Logius voor deze pilot. Het is een verwijzing naar de Haagse Ring waarover het netwerkverkeer van de rijksoverheid loopt. Vanwege technische redenen is de term Haagse Ring ook niet dekkend.

uitgewerkt. In hoofdstuk drie wordt ingegaan op randvoorwaarden ten aanzien van privacy en medezeggenschap die moeten worden ingevuld voordat de pilot van start kan. Hoofdstuk 4 beschrijft de organisatie van de pilot, de planning van de activiteiten en de projectbeheersing en de –risico's. De hoofdstukken vijf, zes en zeven beschrijven achtereenvolgens de projectplanning, projectbeheersing en de projectrisico's. Tot slot is een aan het eind van dit document een korte verklarende woordenlijst opgenomen.

2. Pilot netwerkdetectie Rijksinternet

2.1 Doelstelling van de pilot

Met de pilot netwerkdetectie Rijksinternet wordt een belangrijke stap gezet in het op- en uitbouwen van het Nationaal Detectie Netwerk. De doelstelling van de pilot is als volgt

Onderzoeken en vaststellen of de specifieke dienstverlening van de AIVD en het NCSC, gericht op het netwerkverkeer van de Rijksoverheid, daadwerkelijk bijdraagt aan het tijdig ontdekken van belangrijke digitale dreigingen gericht op die Rijksoverheid.

De bovenstaande doelstelling kan worden onderscheiden in drie subdoelen:

1) ***Beproeven van de effectiviteit, de technische opstelling en bijbehorende werkprocessen***. Met de pilot wordt ondermeer de hardware, systeemconfiguratie en de uitwisselingsprotocollen beproefd. Verder wordt gekeken hoe succesvol de gekozen locatie van de systemen binnen het netwerk is en of de kwaliteit van de indicatoren volstaat. Ook wordt de nodige aandacht gegeven aan de werkprocessen voor beheer- en incidentrespons. Deze ervaringen zijn relevant voor zowel SSC-ICT, AIVD, MIVD als NCSC.

2) ***Vaststellen en beschrijven van de benodigde voorwaarden voor de inrichting van het NDN***. Het idee belangrijke dreigingsinformatie te delen en een actueel situationeel beeld te creëren voor de kritieke infrastructuur is op zich niet uniek. Ervaringen uit de pilot zullen worden vergeleken met ervaringen uit andere initiatieven om zo te komen tot een maatwerk aanpak voor het NDN.

3) ***Organiseren van de samenwerking tussen beoogde NDN deelnemers en belanghebbenden***. Het NDN is voor een belangrijk deel een samenwerkingsvorm waarbinnen gevoelige informatie op basis van vertrouwen wordt uitgewisseld. Op basis van de ervaringen tijdens de pilot kan ook de samenwerking tussen publieke en private organisaties uit de vitale sectoren en defensie-industrie starten en kunnen ervaringen worden gedeeld.

2.2 Opzet van de pilot

In de onderstaande subparagrafen is allereerst het proces beschreven dat tijdens de uitvoering van de pilot operationeel is en wordt vervolgens de technische opstelling nader toegelicht.

2.2.1 Procesbeschrijving tijdens de pilot

De pilot gebeurt op de juridische basis die toestaat het om het Rijksinternet te beveiligen. Vanuit deze grondslag vindt de pilot plaats in opdracht van DGOBR. De AIVD en het NCSC verrichten de detectiewerkzaamheden ieder op hun eigen manier en binnen hun eigen juridische kaders en bevoegdheden.

[redacted] De systemen van de AIVD en het NCSC zijn fysiek en procesmatig van elkaar gescheiden. Er worden in het kader van de pilot geen netwerkgegevens, noch events tussen de AIVD en het NCSC gedeeld. [redacted], behoudt de controle over de informatieprocessen en heeft toegang tot de vastgestelde events. Daarnaast blijven de huidige instrumenten van monitoring van SSC-ICT in productie. Daardoor is het ook mogelijk om het verschil in detectie en de toegevoegde waarde van de extra detectie vast te stellen.

De MIVD richt zich op de dreigingen tegen de nationale veiligheid met een militaire relevantie, zoals cyberspionage jegens de krijgsmacht en de defensie-industrie. Omdat deze pilot zich beperkt tot het civiele Rijks-Internet heeft de MIVD hierin geen expliciete rol, maar draagt met technische en/of juridische kennis bij aan het projectteam NDN. Daarnaast wordt er intensief samengewerkt met de AIVD binnen de gezamenlijke Sigint-Cyber eenheid van de diensten om kennis uit te wisselen en op technisch vlak kennis te ontwikkelen. MIVD is lid van de NDN projectorganisatie en draagt daarmee bij aan het op- en uitbouwen van het NDN. De resultaten van deze pilot zijn van belang voor de verdere ontwikkeling van de detectiewerkzaamheden van MIVD bij de defensie-industrie en het ministerie van Defensie.

In bijlage 1 is de procesbeschrijving van de werkzaamheden voor de AIVD en het NCSC in de pilot verder uitgewerkt.

2.2.2 Technische opstelling tijdens de pilot

De AIVD heeft in de afgelopen jaren ervaring opgedaan met netwerkdetectie in situaties waar de AIVD door organisaties gevraagd is om specifieke ondersteuning te verlenen. Het NCSC heeft een eigen systeem laten ontwikkelen waarmee op de eigen locatie de eerste succesvolle ervaringen zijn opgedaan. Dit systeem wordt nog doorontwikkeld. Tijdens de pilot zullen nieuwe functionaliteiten beschikbaar komen.

Hieronder wordt op hoog abstractieniveau de omgeving weergegeven waar de systemen zich bevinden. Een nadere beschrijving van de technisch opzet van de AIVD en de NCSC systemen en een overzicht van de plaatsing van de systemen zoals beschreven door SSC-ICT is te vinden in bijlage 1.

2.3 Verwachte resultaten

De pilot levert de volgende deelresultaten op:

I. *Een nulmeting.*
Er vindt een analyse plaats van de huidige situatie zoals deze nu bij SSC-ICT is. NCSC en AIVD kijken samen met SSC-ICT naar het aantal en type aanvallen en de gebruikte bronnen. Dit wordt afgezet tegen het type aanvallen en de bronnen die als uitgangspunt dienen voor de pilot. De nulmeting vindt plaats vlak voor de start van de pilot en wordt opgeleverd aan de opdrachtgever van de pilot.

II. *Een maandelijkse rapportage aan SSC-ICT.*
Hierin beschrijven AIVD en NCSC onder meer het aantal aangeboden indicatoren, de technische beschrijving van de indicatoren, de vastgestelde events, de gebruikte (openbare) bronnen en de contactmomenten met SSC-ICT. Met de maandrapportage kan SSC-ICT haar interne rapportage ondersteunen.

III. *Een beproefde infrastructuur met bijbehorende processen en organisatie.*
NCSC en AIVD houden middels een logboek hun ervaringen bij gedurende pilot omtrent onder meer het (technisch) functioneren van de systemen, de ervaringen omtrent het afhandelen van events, incidenten e.d. en het functioneren van de organisatie (beschikbaarheid, bekwaamheid, e.d.). Met deze leerervaringen kunnen beide organisaties bijdragen aan de vorming van het Nationaal Detectie Netwerk.

IV. *Een tussen- en een eindevaluatie.*
Deze evaluaties worden opgeleverd aan de opdrachtgever van de pilot en zijn gebaseerd op:
- de nulmeting (wat verwachten we anders te gaan doen dan nu gebeurt)
- de maandelijkse rapportages (wat stellen AIVD en NCSC vast)
- de terugkoppeling van SSC-ICT (wat is er (anders) vastgesteld door SSC-ICT).
- de ervaringen die uit de logboeks naar voren zijn gekomen.

De tussenevaluatie vindt plaats na drie maanden. De eindevaluatie na zes maanden.

V. *Voortgangsrapportage privacy en medezeggenschap*
In overleg met het RRPF en het OOR wordt afgesproken in welke frequentie en op welke wijze zij gerapporteerd wensen te worden tijdens de uitvoering van de pilot.

VI. *Een beknopte incidentrapportage of incidentrapportages.*
AIVD en NCSC zullen deze aan SSC-ICT aanleveren in het geval van een relevant incident of relevante incidenten tijdens de pilot.

VII. *Een eindrapportage.*
De opdrachtgever wordt geïnformeerd aan het einde van de pilot over onder meer de bevindingen, conclusies en aanbevelingen.

De deelresultaten van de pilot worden gebruikt voor het verder ontwikkelen en uitbouwen van het NDN in 2014.

2.4 Bereik

[redacted]

- De netwerkdetectie activiteiten richten zich alleen op het internetverkeer van / naar de ministeries.
- Het netwerkverkeer blijft op locatie [redacted]
- Na de start van de pilot duurt deze - in ieder geval - zes maanden (up time[3]).

2.5 In werking treden detectie

De AIVD en het NCSC bespreken met SSC-ICT hoe de proefopstelling er uit komt te zien. Op basis van deze informatie is door SSC-ICT een wijzigingsverzoek (RFC) opgesteld. Deze is aan SSC-ICT changemanagement en Logius voorgelegd. Het ontwerp is hierbij getoetst op het niet verstoren van de continuïteit en kwaliteitsborging binnen de architectuurkaders. Logius is akkoord met de opstelling en heeft SSC-ICT de AIVD en het NCSC begeleidt bij het plaatsen van de apparatuur. Vervolgens is door SSC-ICT de aansluitpoorten en de firewalls voor het beheer van de systemen configureren en IP-adressen beschikbaar gesteld.

De apparatuur is in afstemming met de opdrachtgever geplaatst. Echter pas na goedkeuring door DG OBR kan de apparatuur in werking worden gesteld. Tot aan de goedkeuring worden

[3] De periode dat de systemen actief zijn.

alleen de nodige voorbereidingen (testen) uitgevoerd en vinden er geen detectiewerkzaamheden plaats op het netwerk van SSC-ICT met behulp van systemen van de AIVD en het NCSC.

2.6 Operationele randvoorwaarden van de pilot

[redacted]

- SSC-ICT kan beheer uitvoeren op geplaatste systemen en het aanpalende landschap voor zover dat nodig is. Vastgestelde medewerkers van de AIVD en het NCSC hebben in overleg met SSC-ICT toegang tot de geplaatste systemen.
- De systemen van de AIVD en NCSC hebben geen invloed op de werking van de bestaande processen.
- Tijdens de uitvoering van de pilot, kan het gebeuren dat een belangrijk incident zich manifesteert. Hiervoor zijn de bestaande procedures van kracht die gelden bij SSC-ICT en de deelnemende departementen. De AIVD en het NCSC opereren in dat geval binnen de voor hen geldende procedures.
- Aangezien er sprake is van een pilot wordt er gewerkt volgens het principe van vertrouwen en best-effort. Eventuele escalaties worden volgens de overeengekomen governancestructuur afgehandeld.
- De eisen van de opdrachtgever zijn voor aanvang van de pilot helder beschreven.
- Het ontwikkelen van een sector overstijgend dreigingsbeeld zal niet tijdens de pilot gerealiseerd kunnen worden. Hiervoor is de inbreng van de meerdere NDN deelnemers vereist.

3. Medezeggenschap en privacy

Binnen de Rijksoverheid bestaat een breed draagvlak voor het versterken van de weerbaarheid van de Rijksoverheid tegen digitale aanvallen. Het plan van aanpak voor de pilot is ter goedkeuring aangeboden aan het MT DGOBR, de subcommissie informatiebeveiliging (SIB), de interdepartementale commissie CIO's (ICCIO), de interdepartementale commissie bedrijfsvoering Rijk (ICBR) en de minister voor Wonen en Rijksdienst. De geraadpleegde gremia zien het nut en noodzaak voor het uitvoeren van de pilot en adviseren inzichtelijk te maken wat de invloed van de pilot is op de privacy en de rol van de medezeggenschap. Dat past bij een zorgvuldig, bestuurlijk proces om de betrokkenheid van alle belanghebbende te borgen. In de volgende paragrafen wordt eerst ingegaan op de taken en grondslag van de AIVD en het NCSC. Hierna wordt ingegaan op de verwerking van persoonsgegevens en de rol van de ondernemingsraden van de betrokken organisaties.

3.1 Taken, verantwoordelijkheden en waarborgen AIVD

De AIVD verricht op basis van de Wiv 2002 een aantal taken in het belang van de nationale veiligheid, waaronder de zogeheten beveiligingsbevorderende taak. Kern van de beveiligingsbevorderende taak, ook aangeduid als c-taak, is het adviseren over en het bevorderen van beveiligingsmaatregelen. Activiteiten die in het kader van de uitvoering van deze taak worden verricht, zijn gericht op preventie en op het voorkomen dat het belang van de nationale rechtsorde en van andere gewichtige belangen van de staat worden geschaad. De wetgever heeft bij de uitvoering van de c-taak uitdrukkelijk voor ogen gehad dat de uitoefening van deze taak geschiedt in overleg met én met medewerking van de desbetreffende instanties. Belangrijk is dat de inzet van bijzondere bevoegdheden voor de uitvoering van de c-taak niet is toegestaan: bij de activiteiten van de AIVD als onderdeel van deze pilot is van de inzet van bijzondere bevoegdheden, zoals hacken of tappen, dan ook geen sprake.

In de pilot biedt de AIVD aan SSC-ICT een systeem aan die, [redacted] De AIVD heeft via een beveiligde verbinding toegang tot het systeem en kan zo informatie over dreigingen (bijvoorbeeld spionage) toevoegen aan het systeem. Op deze wijze kan in het netwerkverkeer gericht zoeken naar het voorkomen van zo'n dreiging. Indien er een overeenkomst wordt gevonden, wordt deze overeenkomst in het systeem opgeslagen. Alleen de AIVD heeft toegang tot deze overeenkomsten. De AIVD heeft zelf geen inzicht in het achterliggende netwerkverkeer. Periodiek zal de AIVD op gecontroleerde wijze controleren of er overeenkomsten in het systeem zijn opgeslagen. Als dat zo is, zal het SSC-ICT hierover informeren middels een incidentenrapportage. SSC-ICT heeft geen toegang tot het systeem, maar kan de verbinding van het systeem met het netwerkverkeer wel zelfstandig beëindigen.

3.2 Taken, verantwoordelijkheden en waarborgen NCSC

De werkwijze van het NCSC in de beoogde pilot zal zijn dat een systemen (software en hardware) in bruikleen wordt aangeboden aan SSC-ICT. NCSC zal informatie over digitale dreigingen in de systemen aanleveren. SSC-ICT heeft als netwerkbeheerder inzicht in deze informatie. Met de informatie kan op het netwerk dat bij SSC-ICT in beheer is, gezocht worden

naar het voorkomen van de specifieke dreiging. Als er een overeenkomst is tussen de informatie over een dreiging en het netwerkverkeer dan wordt een bevestiging (event) hiervan aan het NCSC verstuurd. Het netwerkverkeer blijft altijd bij de organisatie. NCSC kan na het ontvangen van een bevestiging contact opnemen met SSC-ICT met additionele informatie over de digitale aanval. SSC-ICT kan het NCSC vragen te ondersteunen met onderzoek in het netwerk.

Gezien de aard van de dreigingen (actueel met een verwachte grote impact) is het van belang de informatie zo spoedig mogelijk te delen met SSC-ICT. Het versturen van de dreigingsinformatie naar de systemen en het versturen van de bevestigingen naar NCSC vindt daarom op geautomatiseerde wijze plaats. SSC-ICT behoudt echter regie op de informatieprocessen en kan besluiten ontvangen informatie niet te verwerken en/of bevestigingen niet naar het NCSC te versturen.

De verwerking van gegevens door de organisatie zelf heeft als grondslag de bestaande gedragsregels voor mail en internetgebruik die ieder ministerie heeft opgesteld. Voor de ontvangst en de verwerking van gegevens door het NCSC in een definitief detectienetwerk is door de NCTV vooraf een assessment gemaakt van de juridische en privacy consequenties. Daarbij is geconcludeerd dat op de werkzaamheden van het NCSC de WBP onverminderd van toepassing is. De in artikel 8 van de Wbp genoemde grondslagen voor de verwerking van persoonsgegevens zijn daarbij in het bijzonder de onderdelen 'e' en 'f' van betekenis. Onderdeel 'e' houdt in dat persoonsgegevens mogen worden verwerkt indien dat noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het betrokken bestuursorgaan. [redacted]

3.3 Verwerking persoonsgegevens

In de monitoring van netwerkverkeer en de bijbehorende detectie, komen persoonsgegevens voor. IP-adressen en e-mailadressen zijn hier een voorbeeld van. Het verwerken van persoonsgegevens dient zorgvuldig te gebeuren. De verwerking van persoonsgegevens wordt bezien binnen de kaders van de Wbp.[4] De verwerking als zodanig is noodzakelijk om een op de verantwoordelijke rustende wettelijke verplichting na te komen, namelijk de uitvoering van de verplichting tot beveiliging van persoonsgegevens als bedoeld in artikel 13 van de Wbp.

[4] Er is geen sprake van volledige inzage in het netwerkverkeer.

Ook is voorafgaand aan de pilot het Rijksplatform van Privacyfunctionarissen (RPPF) geraadpleegd. De RPPF heeft geadviseerd een Privacy Impact Assessment (PIA) uit te voeren. Deze PIA is uitgevoerd in samenwerking met de functionarissen gegegevensbescherming van de ministeries BZK en Veiligheid en Justitie. Het resultaat van de PIA wordt besproken met de RPPF. Een belangrijk onderdeel van het werken met persoonsgegevens is de bewaartermijn en de vernietiging van de persoonsgegevens. Deze bewaartermijn is voor de pilot gesteld op 30 dagen. Op de vernietiging van de persoonsgegevens wordt toegezien door de Audit Dienst Rijk (ADR) voor het NCSC, voor de AIVD wordt dit gedaan door de Commissie van Toezicht betreffende de Inlichtingen- en VeiligheidsDiensten (CTIVD).

De melding die SSC-ICT deelt met het NCSC bevat een persoonsgegeven in de vorm van een IP-adres (host en destination). De AIVD controleert periodiek op afstand of er meldingen in haar systemen bij SSC-ICT zijn vastgesteld. Ook deze meldingen bevatten persoonsgegevens (IP-adres, e-mail adres). Andere gegevens die verwerkt worden in het systeem zijn zijn URL's en domeinnamen. Het verwerken van bijzondere persoonsgegevens zoals godsdienst, levensovertuiging, etniciteit, politieke gezindheid, gezondheid en seksuele geaardheid behoren uitdrukkelijk niet tot de persoonsgegevens die verwerkt zullen worden ten behoeve van het nationaal detectie netwerk.

De maatregelen passen in het regime dat bij SSC-ICT reeds van toepassing is op bestaande vergelijkbare strikte beveiligingsmaatregelen om onbevoegden geen toegang te geven. Relevante gegevens die na detectie van een aanval door SSC-ICT worden verstrekt aan de AIVD en het NCSC vallen onder de strikte beveiligingsregimes van deze organisaties. De systemen die aan het NCSC zijn geleverd en de communicatie naar en van deze systemen voldoet aan de vereiste beveiligingsnormen.

De persoonsgegevens op locatie van SSC-ICT en de bevestigingen (events) die aan NCSC worden verstuurd worden 30 dagen bewaard. Na afloop van deze bewaarperiode periode en aan het einde van de pilot worden de gegevens in de systemen van de AIVD en NCSC verwijderd. De ADR en CTIVD zullen op deze verwijderingen toezien.

3.4 Betrokkenheid medezeggenschap in relatie tot de pilot detectie Rijksinternetvoorziening

Gedurende de voorbereiding van de pilot, is overleg tussen BZK, V&J en SZW is geconstateerd dat de pilot een brede casus aanhangig maakt. Beveiligingssoftware wordt beheerd door SSC-ICT of de departementale ICT-beheerorganisatie (in het geval een departement (nog) niet is aangesloten op SSC-ICT). SSC-ICT biedt alleen dienstverlening aan rijksoverheidsorganisaties, de eigenaar van SSC-ICT is DGOBR. Met het onderbrengen van de departementale ICT bij SSC-ICT ontstaat ten aanzien van dit onderwerp een nieuwe situatie indien er wijzigingen optreden in ten aanzien van (het gebruik van) beveiligingssoftware en bestaat er een behoefte aan het harmoniseren van de Internet- en gedragscodes. In de Internet- en gedragscode wordt beschreven op welke wijze medewerkers horen om te gaan met het gebruik van e-mail en Internet. In een dergelijke code wordt vaak melding gemaakt van de persoonsgegevens die worden gelogd en dat gebruik wordt gemaakt van virusscanning om toezicht te kunnen

houden op een veilig gebruik van Internet en e-mail. Gezien het rijksbrede karakter van een geharmoniseerde Internet- en gedragscode, is het OOR het meest aangewezen gremium om de medezeggenschap te organiseren.

Om de Internet- en gedragscodes te harmoniseren voor zover dit de bewerking van persoonsgegevens betreft, wordt voorgesteld de medezeggenschap via het OOR te organiseren. Conform de in het SGO afgesproken werkwijze ten aanzien van de rijksbrede medezeggenschap wordt voorgesteld om SG BZK te mandateren als bestuurder namens alle SG's ten aanzien van de Internet- en gedragscode alsmede de vastlegging van persoonsgebonden gegevens met beveiligingssoftware.

Het netwerkverkeer van de Rijksoverheid wordt beveiligd door SSC-ICT. De pilot is een toevoeging op de bestaande beveiliging. Er wordt ten behoeve van de pilot geen ander netwerkverkeer van medewerkers bewerkt, noch wordt er netwerkverkeer van medewerkers gelogd, anders dan in het geval er sprake is van malafide netwerkverkeer. De pilot richt zich op de beveiliging van het netwerkverkeer van medewerkers met als doel een betere bescherming te kunnen bieden tegen digitale dreigingen.

3.5 Waarborgen zorgvuldige omgang met gegevens

De pilot is beoogd zes maanden (uptime) te duren. Deze duur is nodig om de toegevoegde waarde van de functionaliteit te kunnen aantonen. Indien de opdrachtgever (DG OBR) dit wenselijk acht, kunnen de systemen op elk moment tijdens de pilot door SSC-ICT worden gedeactiveerd en zullen AIVD en NCSC geen toegang meer hebben tot de systemen en geen informatie meer kunnen uitwisselen. Het verwijderen van systemen op de locatie van het SSC-ICT is betrekkelijk eenvoudig en kan door SSC-ICT worden gerealiseerd. Het vernietigen van gegevens zal plaatsvinden volgens de afgesproken procedures. De ADR en CTIVD kan toezicht houden op deze procedures. De pilot is daarmee omkeerbaar. De opdrachtgever kan daartoe besluiten zonder afhankelijk te zijn van de AIVD en het NCSC.

Zoals hiervoor aangegeven verwerken AIVD en NCSC persoonsgegevens. Waar het het IP-adres betreft kunnen deze organisaties niet zelfstandig achterhalen welke medewerker bij een IP-adres hoort. SSC-ICT kan dit vanuit haar beveiligingstaak wel. In geval van een incident kan het nodig zijn dat SSC-ICT weet welke werknemer hier bij betrokken is. Tussen SSC-ICT en AIVD en NCSC worden geen werknemergegevens uitgewisseld. ADR en CTIVD zal gevraagd worden hierop toe te zien. Het OOR zal middels een rapportage over de voortgang tijdens de pilot geïnformeerd worden.

4. Organisatie van de pilot

De minister van V&J heeft opdracht gegeven tot het realiseren van het Nationaal Detectienetwerk (NDN). Hiervoor is een stuurgroep NDN ingericht. De stuurgroep is verantwoordelijk voor de sturing op het totaal van activiteiten dat plaatsvindt in het kader van NDN. De pilot netwerkdetectie Rijksinternet is één van die activiteiten. Voor de pilot wordt een aparte governance ingericht omdat de opdrachtgever van de pilot een andere is dan die van het NDN.

4.1 Governance pilot

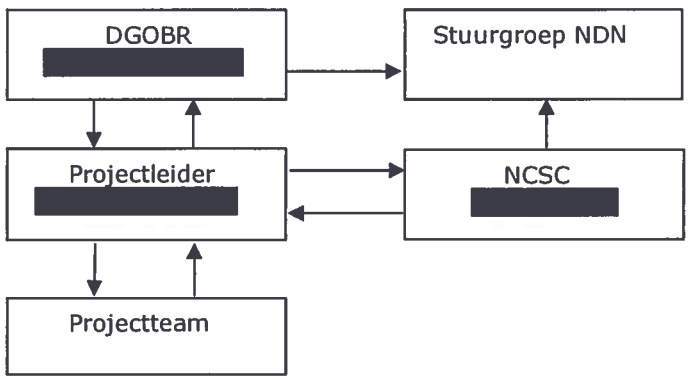
DGOBR is de eigenaar van de Rijksinternetkoppeling waar detectie in het kader van de pilot zal plaatsvinden. DGOBR heeft de taak te zorgen voor veilig dataverkeer van overheidsorganisaties, dat loopt via de Rijksinternetkoppeling. Vanwege deze taak is de DGOBR opdrachtgever van de pilot netwerkdetectie Rijksinternet. Opdrachtnemers zijn de AIVD, MIVD en het NCSC, waarbij het NCSC optreedt als hoofd opdrachtnemer.

- Dagelijkse besturing van de pilot

Ten behoeve van de voorbereiding en exploitatie van de pilot netwerkdetectie Rijksinternet wordt voor de governance de volgende organisatie ingericht.

1) *Gedelegeerd opdrachtgever voor de pilot*: [redacted] werkzaam bij DGOBR en lid van de stuurgroep NDN. De gedelegeerd opdrachtgever is samen met de gedelegeerd opdrachtgever voor het NDN [redacted], contactpersoon voor de projectleider van de pilot en zorgt voor de verbinding met de stuurgroep NDN. Deze zorg bestaat er onder andere uit dat de stuurgroep NDN wordt geïnformeerd over die aspecten van de pilot die van invloed zijn op het verder ontwikkelen van het NDN. Voorbeeld hiervan is terugleggen van de resultaten van de pilot in de stuurgroep. De gedelegeerd opdrachtgever neemt aan het eind van de pilot de resultaten in ontvangst en verleent decharge aan de projectleider.
2) *Projectleider*: [redacted]. De projectleider is verantwoordelijk voor de opzet, het verloop en de resultaten van de pilot. De projectleider informeert tweewekelijks de gedelegeerd opdrachtgever over de voortgang van de pilot en stuurt tevens het projectteam taakgericht aan. Ook organiseert de projectleider benodigde overleggen, o.a. met het projectteam. Tevens is de projectleider verantwoordelijk voor het opleveren van de resultaten aan de (gedelegeerd) opdrachtgever.
3) *Projectteam*: deskundigen van de AIVD, MIVD, NCSC en DGOBR. Het projectteam is verantwoordelijk voor het uitvoeren van taken die een bijdrage leveren aan de resultaten. Deze taken lopen uiteen van het doen van voorstellen en deze uitvoeren, tot het beantwoorden van juridische vragen en communiceren over de pilot. Het projectteam werkt onder leiding van de projectleider en voert in dat kader maandelijks overleg. Als platform voor dit overleg zal de reeds bestaande NDN klankbordgroep worden gebruikt. Hierin zitten nu medewerkers van AIVD, MIVD en NCSC.

Ten behoeve van de pilot zal de klankbordgroep worden uitgebreid met een vertegenwoordiger uit DGOBR.



Governance pilot

4.2 Melden van detectie aan pilot departementen

AIVD en NCSC melden alle mogelijke beveiligingsincidenten aan de beveiligingsverantwoordelijke van SSC-ICT. Deze laatste bepaalt op basis van bestaande protocollen hoe de melding verwerkt moet worden. SSC-ICT kan besluiten op basis van de melding en rapportage de ICT-beveiligingsverantwoordelijke te informeren van het getroffen netwerksegment (een ministerie). Afhankelijk van de ernst van het mogelijke beveiligingsincident vindt de melding aan SSC-ICT direct na vaststelling plaats of maandelijks tijdens de rapportageperiode. De melding aan SSC-ICT omvat een rapportage waarin technische indicatoren zijn opgenomen.

Op basis van informatie in de rapportage is de beveiligingsverantwoordelijke in staat om verder onderzoek te doen. Door informatie te correleren met gegevens uit logging van bijvoorbeeld een proxy-, mail- en/of DNS-server, kan door de beveiligingsverantwoordelijke zelfstandig verdere duiding aan het incident worden gegeven. Zoals eerder aangegeven kunnen de AIVD en het NCSC kunnen indien gevraagd ook in het verdere onderzoek ondersteuning bieden.

Zowel de AIVD en het NCSC beschikken nu al over een gestandaardiseerd proces waarin een organisatie geinformeerd kan worden over een mogelijk beveiligingsincident. NCSC heeft daarnaast vanuit bestaande werkzaamheden al een werkrelatie met SSC-ICT. Het melden van mogelijke beveiligingsincidenten door AIVD en NCSC aan de beveiligingsverantwoordelijke van SSC-ICT, zal naar verwachting op de volgende punten afwijken:

- Via het systeem van NCSC heeft de beveiligingsverantwoordelijke van SSC-ICT zelf een incident opgemerkt en start het bestaande responsproces;
- Via het systeem van NCSC is een mogelijk beveiligingsincident vastgesteld, welke (nog) niet is opgemerkt door de beveiligingsverantwoordelijke van SSC-ICT. Afhankelijk van de vermoedde ernst kan NCSC n.a.v. de ontvangen berichtgeving (event) de verantwoordelijke direct of tijdens de maandelijkse rapportage hierover informeren.

- Via het systeem van de AIVD is een mogelijk beveiligingsincident vastgesteld. Afhankelijk van de vermoedde ernst kan de AIVD de verantwoordelijke direct of tijdens de maandelijkse rapportage hierover informeren.

4.3 Besluitvorming over de pilot

De besluitvorming over de pilot verloopt tweeledig. Enerzijds is de stuurgroep NDN betrokken vanuit de eindverantwoordelijkheid voor het NDN. De resultaten van de pilot worden met de stuurgroep gedeeld via DGOBR en vormen de basis voor het bepalen van vervolgstappen voor NDN. Het bepalen van de vervolgstappen is de verantwoordelijkheid van de stuurgroep NDN. Voor het gebruik van resultaten uit de pilot in die vervolgstappen, moet voorafgaand aan de pilot afspraken worden gemaakt met DGOBR als opdrachtgever. Anderzijds verloopt besluitvorming over de start, de exploitatie en de resultaten van de pilot via de dg OBR, de subcommissie informatiebeveiliging, de ICCIO en het ICBR. Zij hebben inmiddels ingestemd met het plan van aanpak voor de pilot en worden ingeschakeld bij (belangrijke) wijzigingen in de pilot en toetsen of de vooraf afgesproken resultaten zijn behaald.

4.4 Investeringsanalyse

Voor 2013 heeft de Stuurgroep NDN besloten geen financiële claims te doen voor de pilot. De benodigde middelen worden uit de bestaande begrotingen gefinancierd, eventueel door interne prioriteitstelling binnen de deelnemende organisaties.

De volgende investeringen vinden plaats:
- De DG OBR investeert met inzet van mensen.
- De AIVD investeert met middelen en inzet van mensen.
- De MIVD investeert met inzet van mensen.
- Het NCSC investeert met middelen en inzet van mensen.
- SSC-ICT belast de inzet van mensen door
- Logius belast de inzet van mensen door

Uitgangspunt bij deze investeringsanalyse is dat de reguliere werkzaamheden van SSC-ICT (beheren, verwerken meldingen, responsactiviteiten uitvoeren etc.) niet worden doorberekend, maar behoren tot het takenpakket van SSC-ICT.

Aan het eind van de pilot wordt besloten of de pilot voldoende meerwaarde heeft bewezen en of de detectie structureel wordt ingericht en zo ja, op welke wijze. Dit gebeurt aan de hand van de rapportages zoals beschreven in hoofdstuk 6. Dan zal ook bekend zijn welke bedragen hiermee zijn gemoeid en wat er eventueel aan departementen wordt doorberekend in de toekomst wanneer het NDN wordt uitgebouwd. In de voorbereiding en tijdens de uitvoering van pilot zullen in dit kader de verschillende werkzaamheden onderscheiden en nader ingeschat worden.

4.5 Communicatie over de pilot

De stuurgroep NDN is eindverantwoordelijk voor de interne en externe communicatie over het NDN. [redacted] Voorgesteld wordt communicatiedeskundigen van de AIVD, DCS/NCSC en DGOBR hiervoor te laten samenwerken. Deze interdepartementale groep communicatiedeskundigen stemt het communicatieproces voor de start van de pilot af aan de hand van de uitgangspunten van het voorstel voor de pilot netwerkdetectie Rijksinternet. De communicatiedeskundigen zijn verantwoordelijk voor het opstellen en de uitvoering van de beleidscommunicatie.

5. Planning

5.1 Randvoorwaarden

- De start van de pilot hangt af van het akkoord van DGOBR en ICCIO.
- De OOR wordt vooraf geïnformeerd en betrokken bij de uitvoering en afronding van de pilot.
- De ADR en de CTIVD zullen toezicht houden op de met de OOR en het RPPF afgesproken procedures.
- Er is voldoende deskundige capaciteit beschikbaar in het projectteam om de werkzaamheden uit te voeren.
- De pilot loopt door in 2014. Voor dit deel zullen deelnemende organisaties nog steeds investeren op basis van de gemaakte afspraken.
- De planning is opgesteld er van uitgaande dat er geen verstoring plaats zou vinden naar aanleiding van een groot incident. Indien een verstoring plaatsvindt, moet op dat moment worden bekeken welke invloed dit heeft op de pilot.

5.2 Mijlpalenplanning

Het verloop van de pilot kan worden beschreven aan de hand van drie fasen. In de *voorbereidingsfase* worden alle belanghebbenden en hun rol in de pilot bekend. Er komt een goed beeld van hoe de proefopstelling er uit gaat zien en welke vraagstukken er zijn. De nodige consultaties worden uitgevoerd. Het ambtelijke proces wordt voorbereid en wordt doorlopen. Het wijzigingsproces (RFC) dat voorafgaat aan de exploitatie wordt doorlopen en afgerond. In de *exploitatiefase* werken SSC-ICT, AIVD en NCSC samen in het proces dat in het voorstel voor de pilot is beschreven. Er vinden verschillende evaluaties plaats gedurende de exploitatie. Over de voortgang wordt volgens de afgesproken wijze gerapporteerd. In de *opleveringsfase* worden de eindresultaten beschreven en gerapporteerd. De proefopstelling wordt volgens afspraken opgeleverd.

De planning van de pilot wordt hieronder aan de hand van mijlpalen beschreven.

	Mijlpalen	Status
2	VOORBEREIDINGEN PILOT	
3	Plan van aanpak pilot opgeleverd	gereed
4	Plan van aanpak pilot geaccordeerd door DGOBR, SIB, ICCIO, ICBR	gereed
5	Netwerk detectie systemen beschikbaar bij AIVD, NCSC	gereed
6	Impact technische infrastructuur bepaald door Logius en SSC-ICT	gereed
7	Voorbereidingen op locatie SSC-ICT uitgevoerd	loopt
8	Opleveren privacy impact assessment i.s.m. RPPF	loopt
9	Betrekken medezeggenschap organen	loopt
10	Nulmeting	open
11	GO opdrachtgever	open
12	EXPLOITATIE PILOT	
13	Start pilot	open
14	Maandelijkse rapportage	open
15	Evaluatie ervaringen AIVD/NCSC	open
16	Tussenevaluatie aan opdrachtgever	open
17	Eindevaluatie aan opdrachtgever	open
18	Eindrapportage	open
19	Decharge	open

6. Beheersing

6.1 Go/No-go

De gedelegeerd opdrachtgever voor de pilot kan in overleg met de stuurgroep NDN besluiten de pilot te continueren of (tijdelijk) te stoppen na:

- het bereiken van een mijlpaal;
- een tijdsoverschrijding van meer dan 10%;
- een substantiële (verwachte) toename van meerwerk;
- het uitblijven van relevante bevindingen na zes maanden (up time);
- het voorkomen van een grootschalig incident.

6.2 Voortgangsrapportage

Door DG OBR wordt een rapportagesjabloon beschikbaar gesteld waarmee de projectleider tweewekelijks aan de gedelegeerde opdrachtgever rapporteert over de resultaten van de pilot.

De stuurgroep NDN geeft aan op welke wijze de gedelegeerd opdrachtgever tweemaandelijks over de voortgang van de pilot dient te rapporteren.

De projectleider zal samen met het projectteam en de gedelegeerde opdrachtgever de tussen- en eindevaluatie, de eindrapportage en de beknopte incidentrapportage SMART maken.

6.3 Kwaliteitsborging

- NCSC werkt de uitkomsten van de privacy impact assessment uit voor haar systemen, processen en organisatie.
- De ADR en CTIVD worden gevraagd de naleving van de met de OOR en het RPPF afgestemde waarborgen te evalueren.
- Medewerkers van de AIVD en het NCSC die bij de pilot betrokken zijn, hebben allen een beveiligingsonderzoek (screening) ondergaan.
- Slechts een klein team van medewerkers van de AIVD is betrokken bij het controleren op gebeurtenissen (events) in het AIVD systeem.
- Alleen NCSC medewerkers die vanuit hun taak verantwoordelijk zijn voor het behandelen van incidenten kunnen met events vanuit de pilot in aanraking komen.
- De verwerking van events bij NCSC vindt plaats volgens een gestandaardiseerd proces, gericht op het waarborgen van de betrouwbaarheid, integriteit en vertrouwelijkheid van de informatie.
- Er wordt zoveel als mogelijk gebruik gemaakt van de bestaande werkprocessen en protocollen bij AIVD, NCSC en SSC-ICT.
- SSC-ICT, de opdrachtgever DGOBR en de OOR zullen middels rapportages geïnformeerd worden over de bevindingen in en de voortgang van de pilot.

6.4 Oplevering en vervolg

Bij oplevering van de pilot worden de volgende resultaten opgeleverd aan de gedelegeerd opdrachtgever:

- een tussen- en een eindevaluatie op basis van vooraf opgestelde criteria;
- een beproefde infrastructuur met bijbehorende processen en organisatie;
- een eindrapportage met onder meer de bevindingen, conclusies, aanbevelingen;
- een incidentrapportage of incidentrapportages in het geval van een relevant incident of relevante incidenten tijdens de pilot.

In de eindrapportage zijn onder meer de antwoorden opgenomen op de volgende specifieke vragen van de opdrachtgever:

1. Is aantoonbaar dat de rijksoverheid door de detectie veiliger wordt?
2. Worden door de detectie signalen eerder zichtbaar dan nu het geval is?
3. Worden betrokken organisaties voldoende geïnformeerd?
4. Laat de pilot zien dat deze wijze van detectie standaard moet worden ingevoerd?

In de eindrapportage wordt een advies gegeven aan de gedelegeerd opdrachtgever over het vervolg van de pilot. De gedelegeerd opdrachtgever bespreekt dit advies met de NDN stuurgroep. Indien een vervolg gewenst is kunnen zij hiertoe besluiten, in afstemming met DGOBR, SIB en ICCIO wanneer dit vereist is.

7. Projectrisico's

Gebeurtenis	Tegenmaatregel	Kans	Impact	Risico
[redacted]	[redacted]			
De verhuizing van SSC-ICT rond december 2013 betekent op zijn minst een tijdelijke stop voor de pilot. Het is niet bekend wat precies de gevolgen gaan zijn in termen van kosten, techniek en tijd.	Bij het wijzigingsproces meenemen hoe de verhuizing geregeld gaat worden en welke gevolgen dit heeft voor de pilot.			
De specifieke dreigingsinformatie die de AIVD en het NCSC aanleveren is heel specifiek en zeker niet alledaags. Dit kan betekenen dat bevindingen beperkt zijn of dat lang uitblijven.	De opdrachtgever en de stuurgroep geven de pilot voldoende tijd om de toegevoegde waarde aan te tonen.			
Er kan tijdens de pilot nog geen sectoroverschrijdend beeld van dreigingen en incidenten getoond worden, waarmee een deel van de toegevoegde waarde niet aangetoond kan worden.	Vanuit het project wordt aan de hand van andere initiatieven getoond hoe een dergelijk beeld er uit ziet.			
In de media wordt negatief gecommuniceerd over detectie in het algemeen of over de pilot specifiek wat deelnemende ministeries terughoudend maakt.	Er wordt bij de start van de pilot helder en transparant gecommuniceerd over de pilot naar betrokken organisaties			

Kans en Impact scores
1 = lage kans op voorkomen / kleine verwachte impact
2 = middelhoge kans op voorkomen / middelgrote verwachte impact
3 = grote kans op voorkomen / grote verwacht impact

Verklarende woordenlijst

CERT	Computer Emergency Respons Team. NCSC vervult als GovCERT een tweedelijns ondersteuning aan de Rijksoverheid.
Diginotar	In september 2011 bleek dat het bedrijf DigiNotar was gehackt en dat frauduleuze certificaten zijn gegenereerd. De certificaten waren ook bij de Nederlandse overheid in gebruik. Naar aanleiding van de hack is het vertrouwen in DigiNotar opgezegd. Als gevolg hiervan moesten duizenden certificaten worden vervangen, bestaande DigiNotar certificaten worden ingetrokken, software updates van bijvoorbeeld browsers en operating systems geïnstalleerd. Binnen de overheid is dit als een crisis opgeschaald, inclusief opschaling bij het NCC.
Dorifel	In 2012 zijn diverse overheidsinstellingen, universiteiten en bedrijven in Nederland besmet geraakt met een virus dat MS Excel en Word documenten door een bestand met het virus. Het virus richtte zich op het verkrijgen van persoonlijke informatie, het verwijderen van bestanden en op het inzetten van een computer voor andere aanvallen.
DDoS	Afkorting voor distributed denial-of-service. Een poging van kwaadwillenden om met meerdere computers tegelijk een aanval uit te voeren op een systeem om zo een computere, network of dienst onbeschikbaar te maken.
Event	Een event is een gebeurtenis die wordt vastgesteld wanneer er een overeenkomst is tussen de technische beschrijving van een mogelijke dreiging (malware, spionage e.d.) en het netwerkverkeer bij SSC-ICT. Een event is dus niet het netwerkverkeer zelf. In een event kan informatie worden opgeslagen zoals datum en tijd waarop het event is vastgesteld, IP adres MAC adres en poortnummer van het verzendende systeem, indicatie van de dreiging.
NDN	Het geheel van systemen, processen, mensen en organisaties, dat gericht is op het verzamelen en delen van dreigingsinformatie, op het aanbrengen van samenhang in die dreigingsinformatie en op het delen van een situationeel beeld met de deelnemers aan het NDN.

Bijlagen

Bijlage 1 Generiek procesbeschrijving

Bijlage 2 Organisaties aangesloten bij het Overleg Orgaan Rijk (OOR)

1. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
2. Ministerie van Buitenlandse Zaken
3. Ministerie van Algemene Zaken
4. Ministerie van Economische Zaken
5. Ministerie van Financiën
6. Ministerie van onderwijs, Cultuur en Wetenschap
7. Ministerie van Sociale Zaken en Werkgelegenheid
8. Ministerie van Infrastructuur en Milieu
9. Ministerie van Volksgezondheid, Welzijn en Sport
10. Concern ondernemingsraad Belastingdienst