VERDONCK KLOOSTER & ASSOCIATES

DE ROL VAN DIGINETWERK BIJ VEILIGE INFORMATIE-UITWISSELING

Op welke wijze kan Diginetwerk een bijdrage leveren aan veilige informatie-uitwisseling binnen de overheid?

VERDONCK KLOOSTER & ASSOCIATES

DE ROL VAN DIGINETWERK BIJ VEILIGE INFORMATIE-UITWISSELING

Op welke wijze kan Diginetwerk een bijdrage leveren aan veilige informatie-uitwisseling binnen de overheid?

Joep Janssen, Onno Massar en Erik Mark Meershoek

DATUM	30 december 2012
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20120515

MANAGEMENTSAMENVATTING

De doelstelling van dit onderzoek is een samenhangend beeld te schetsen van Diginetwerk in relatie tot veilige informatie infrastructuur/architectuur bij de overheid.
Daarbij is een antwoord gegeven op de volgende vier hoofdvragen:

a. Wat zijn gebleken belangrijke randvoorwaarden bij een veilige infrastructuur voor informatie-uitwisseling?
b. Op welke wijze draagt Diginetwerk (in relatie tot andere voorzieningen) bij aan een veilige infrastructuur voor informatie-uitwisseling binnen de overheid?
c. Waar bevinden zich de belangrijkste risico's ten aanzien van veilige informatie-uitwisseling?
d. Gelet op belangrijke randvoorwaarden: welke aanknopingspunten zijn er voor verbetering van de huidige beveiligingsinfrastructuur in termen van kosten en verantwoordelijkheden?

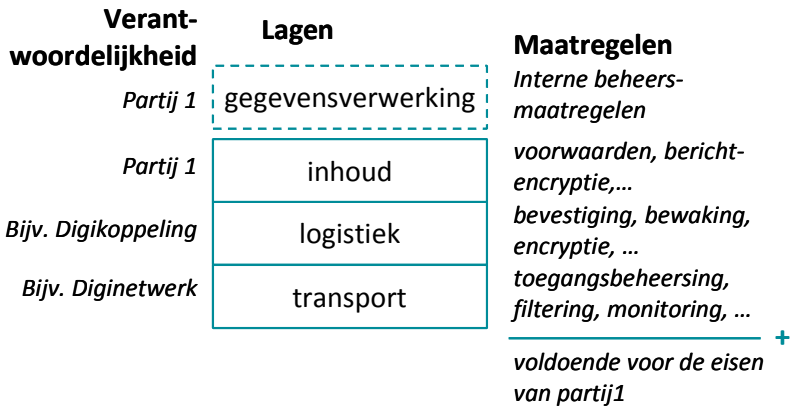
In het onderzoek is aangesloten bij algemeen geaccepteerde kaders voor het beheer en de beveiliging van generieke ICT infrastructuren voor de overheid.

Uit het onderzoek komt het volgende beeld naar voren:

a. Belangrijke randvoorwaarde voor veilige informatie-uitwisseling zijn de eisen die de stakeholders stellen aan beveiligingsmaatregelen van informatie-uitwisseling. Organisaties met een publieke taak die op een geautomatiseerde wijze persoonsgegevens verwerken en uitwisselen hebben een wettelijke verplichting (Wet Bescherming Persoonsgegevens) tot het beveiligen van persoonsgegevens. Dit geldt ook voor de beherende partijen van Diginetwerk en de externe leveranciers van netwerkdiensten.
   De wet eist dat deze organisaties passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen. Dit begint bij de verwerkingsprocessen van de betrokken stakeholder organisaties en in de applicaties die deze processen ondersteunen. Vervolgens worden maatregelen getroffen op de koppelvlakken (zowel op het niveau van applicaties als op het niveau van bijvoorbeeld Digikoppeling). De beveiliging van het netwerk kan daar ook een bijdrage aan leveren aan de totale beveiliging.
   Een andere belangrijke randvoorwaarde is een evenwichtige verdeling van strategische, tactische en operationele regievoering van Diginetwerk.
   Voor het strategisch beheer door het ministerie van BZK zijn geen rollen en verantwoordelijkheden gedefinieerd en ingevuld. Dit houdt ook in dat de IT-governance van Diginetwerk niet is ingevuld. Er vindt geen bestuurlijke afstemming plaats over het strategisch beleid. Er is geen sourcingstrategie ontwikkeld voor de marktpartijen die betrokken zijn bij Diginetwerk. Er is geen bestuurlijk beveiligingsbeleid geformuleerd en er vindt geen bestuurlijk toezicht en verantwoording plaats over de naleving van beleids- en beveiligingsregels.
   Het tactisch beheer van Diginetwerk is belegd bij Logius.

Over het operationeel beheer is tussen Logius en BKWI een samenwerkingsovereenkomst gesloten.

b. Diginetwerk levert een bijdrage aan de veilige informatie-uitwisseling door het treffen van beveiligingsmaatregelen op de zogenaamde "transportlaag".
De functies voor informatie-uitwisseling zijn te verdelen in een drietal “infrastructuur lagen”. De onderste laag, transport, omvat het datanetwerk dat wordt gebruikt. De tweede laag “logistiek” omvat de functies die nodig zijn om de gegevens in voor de applicatie handzame eenheden, bijv. bestanden, berichten, webpagina’s, over te brengen. De derde laag bevat functionaliteit om de inhoud van de berichten te borgen. Hier worden de bestanden of berichten samengesteld en gelezen. In deze laag horen afspraken thuis over betekenis van gegevens. In deze laag kan ook worden geborgd dat de gegevens conform gemaakte afspraken worden uitgewisseld.



Elke partij neemt in het eigen domein maatregelen en stelt eisen aan de maatregelen over verschillende lagen van de infrastructuur. Deze eisen komen tot stand op basis van een risicoanalyses en onderling overleg. Op basis hiervan kan vervolgens een onderbouwde keuze gemaakt worden voor invulling van de beveiliging van de transportlaag, waar Diginetwerk zich bevindt.
Binnen Diginetwerk worden de volgende beveiligingsmaatregelen getroffen.

		Maatregel	Verantwoordelijkheid
Beschikbaarheid	B1	Redundantie in netwerkcomponenten, verbindingen en aansluitingen van koppelnetwerken.	Beheerder(s) Diginetwerk & Koppelnetwerk Optioneel: beheerders bedrijfsnetwerk
	B2	Procedures en tools om in geval van storingen de oorzaak snel te achterhalen.	Gezamenlijke verantwoordelijkheid, vnl. beheerders Diginetwerk en Koppelnetwerken.
Exclusiviteit	E1	Dienst is alleen beschikbaar voor organisaties met toegang tot Diginetwerk.	Beheerder(s) Diginetwerk & Koppelnetwerken
	E2	Alleen bekende organisaties wordt toegang verleent tot Diginetwerk ("besloten" netwerk).	Beheerders Koppelnetwerken
	E3	Alleen verkeertype HTTP(s), poort 443, doorgelaten.	Beheerder Diginetwerk
	E4	Diginetwerk is gescheiden van het Internet.	Beheerders Koppelnetwerken & Bedrijfsnetwerken
Integriteit	I1	Zie E4.	
	I2	Bescherming tegen "ongewenst verkeer" (hackers, virussen, spyware, spam).	Beheerders Bedrijfsnetwerken

c. Stakeholders noemen de volgende belangrijke risico's bij veilige informatie-uitwisseling:
   1. Non-compliance (leidend tot juridische en/of politieke schade) aan de eisen van alle voor deelnemers geldende wet- en regelgeving.
   2. Discontinuïteit van de (e-)overheid. Een groot aantal services van de (e-) overheid kunnen uitvallen als bijvoorbeeld basisregistraties niet toegankelijk zijn om basisgegevens op te halen.
   3. Chaos door georganiseerde misdaad of cyberterroristen. Cyberterroristen kunnen uit politieke motieven of uit onvrede met overheidshandelen besluiten om verwarring te creëren.
   4. Fraude door manipulatie (belasting, toeslagen). Fraude wordt veelal mogelijk gemaakt door processen te manipuleren en misbruik te maken van gebrekkige controles.
   5. Aftappen van verkeer (bij netwerkprovider, etc.). Dit tast de privacy van de personen aan die deze gegevens betreffen.
   6. Misbruik / stelen van uitgewisselde gegevens bij een minder goed beveiligde afnemer.
   7. Sluipende aantasting van de belangen van de burger door opstapeling van minieme datalekken als gevolg van het massale gebruik van elektronische informatie-uitwisseling.
   8. Sluipende aantasting van de belangen van de overheid.
      Hetzelfde gevaar loopt de overheid. Spionage betreft vaak het verzamelen van zeer veel gegevens waaruit de tegenstander door analyse geheimen kan onthullen.
   9. Inbreuken worden niet gedetecteerd doordat beheer niet in één hand ligt.
      Om inbreuken op de beveiliging te constateren, moet de beheerder van een netwerk of systeem dit goed monitoren en de monitoring gegevens regelmatig analyseren.

   De stakeholders vinden beveiliging van de informatie-uitwisseling van groot belang. Zij gaven aan geen concreet beeld te hebben hoe de afweging tussen beveiliging en gebruikersgemak te

kunnen maken. Daarom kiest men er veelal voor de geldende normen en regels nauwkeurig te volgen.
Enkele stakeholders pleitten voor het instellen van audits om partijen toe te laten tot een besloten overheidsnetwerk zoals Diginetwerk.

d. Aanknopingspunten voor verbetering van de huidige beveiligingsinfrastructuur moeten vooral gezocht worden in het definiëren van strategische (beveiligings-) beleidskaders voor Diginetwerk. Verder is het van belang in goed onderling overleg en op basis van een risicoafweging gezamenlijk eisen stellen aan het beveiligingsniveau van de uit te wisselen informatie en de daarbij te nemen beveiligingsmaatregelen.

Hiervoor staan 3 scenario's open:

Scenario	Omschrijving
1. Federatief	Dit scenario komt overeen met de huidige situatie (verschillende netwerken, waaronder Diginetwerk, met verschillende kenmerken). Beveiliging van de informatie-uitwisseling vindt op verschillende lagen plaats, afhankelijk van het toepassingsgebied. Dit vereist intensief collegiaal overleg tussen de ketenpartners.
2. Centraal	Eén netwerkvoorziening voor de overheid. Eén voorziening wil overigens niet zeggen dat dit ook (fysiek) één netwerk is. Wel is in dit scenario sprake van strakke centrale regievoering, verantwoording en toezicht. Door centrale regie, beheer in één hand wordt het mogelijk in dit scenario een groot aantal beveiligingsmaatregelen in de transportlaag te treffen.
3. Internet	Gebruik van Internet. In dit scenario wordt veruit het grootste deel van de informatie via het Internet uitgewisseld. Alleen voor hoog risico informatie-uitwisseling (zoals bijvoorbeeld staatsgeheime informatie) wordt nog gebruik gemaakt van private verbindingen en/of besloten netwerken. Beveiliging van de informatie-uitwisseling zal in hoge mate steunen op maatregelen op de logistieke en op inhoud laag. Door de open aard van Internet is de kans dat de aangesloten systemen worden aangevallen, zeer hoog.

Een afweging tussen de voor- en nadelen van de scenario's kan uit oogpunt van informatiebeveiliging worden gemaakt door het uitvoeren van een business risicoanalyse,

waarin op basis van de eisen die door de stakeholders gesteld worden aan de informatiebeveiliging, en in samenhang met de lagen inhoud en logistiek, de beveiligingsmaatregelen voor de voor Diginetwerk bepaald worden.

Daarbij is informatiebeveiliging niet het enige criterium. Andere criteria zijn: kosten, zorgen voor gezonde marktwerking, algemene beleiduitgangspunten zoals "gebruik generieke e-overheidsvoorzieningen" en de risico's voor het functioneren van de overheid als geheel bij uitval van de onderliggende infrastructuur.

INHOUDSOPGAVE

1 AANLEIDING

De afdeling Informatiebeleid van het ministerie van BZK/DGBK/beleidsdirectie B&I wil graag een beter beeld krijgen van de randvoorwaarden voor veilige informatie-uitwisseling van overheidspartijen. Anno 2012 spelen diverse voorzieningen (bijvoorbeeld Diginetwerk) daarbij een rol. Diginetwerk is ontwikkeld binnen het programma Bundeling Landelijke Netwerken (onderdeel van Programma Andere Overheid). Bij de overdracht naar beheer is echter geen structurele financiering overgedragen waardoor nu discussie is over het eigenaarschap en de financiering van Diginetwerk. Om tegemoet te komen aan de bestuurlijke wens om meer duidelijkheid en besluitvorming is meer kennis op dit terrein cruciaal.
Behoefte bestaat aan een samenhangende visie de huidige situatie, de eisen en wensen, alsmede de technologische ontwikkelingen op het gebied van veilige informatie-uitwisseling binnen de overheid en de rol van de verschillende e-overheidsvoorzieningen, om van daaruit afgewogen bestuurlijke besluiten rond Diginetwerk te kunnen nemen. Specifieke aandacht vraagt de rol- en verantwoordelijkheidsverdeling rondom Diginetwerk en de rol van B&I daarbij (governance).

Daarbij is enerzijds behoefte aan een beleidsmatige ”helikopterblik" op het "waarom" en het "wat" van de veilige informatie-uitwisseling binnen de overheid en anderzijds een gedetailleerde analyse van de uitvoering (het "hoe"en "waarmee") van de veilige informatie-uitwisseling.
Op basis van de bevindingen uit deze analyse kan de opdrachtgever waar nodig en gewenst aanpassingen en verbeteringen in beleid en uitvoering formuleren.

2 DOELSTELLING, SCOPE EN WERKWIJZE

2.1 Doelstelling

De doelstelling van het onderzoek is een samenhangend beeld te schetsen (een "foto") van Diginetwerk in relatie tot veilige informatie infrastructuur/ architectuur. Dit omvat de volgende elementen:

- Diginetwerk in de huidige opzet;
- de verschillende onderliggende (rijks-)netwerken;
- visievorming die gaande is in kavel 7 (Basisinfrastructuur) van de generieke ICT diensten Rijk;
- relevante aanpalende netwerken;
- relaties met netwerken van private partijen, zoals Gemnet;
- andere voorzieningen zoals Digikoppeling; PKI certificaten en een eventueel nieuw te benutten overheidseigen Top Level Domein (TLD).

Naast bovenstaande punten neemt VKA bij de schets ook de visievorming rondom beveiliging van overheidsnetwerken mee, zoals ontwikkeld in het NORA 'Dossier Informatiebeveiliging' en in de 'Patronen Informatiebeveiliging' van het Platform Informatiebeveiliging, waarin uitgebreid ingegaan wordt op de beveiliging van overheidsnetwerken en de rol van koppelvlakken daarbij.

2.2 Vraagstelling

VKA beantwoordt de volgende vier hoofd onderzoeksvragen:

a. Wat zijn gebleken belangrijke randvoorwaarden bij een veilige infrastructuur voor informatie-uitwisseling?
b. Op welke wijze draagt Diginetwerk (in relatie tot andere voorzieningen) bij aan een veilige infrastructuur voor informatie-uitwisseling binnen de overheid?
c. Waar bevinden zich de belangrijkste risico's ten aanzien van veilige informatie-uitwisseling?
d. Gelet op belangrijke randvoorwaarden: welke aanknopingspunten zijn er voor verbetering van de huidige beveiligingsinfrastructuur in termen van kosten en verantwoordelijkheden?

De beantwoording van bovenstaande onderzoeksvragen moet inzicht geven of voort gegaan kan worden op de ingeslagen weg of dat bijstelling nodig is.

2.3 Scope

Tot het onderzoek behoort WEL	Tot het onderzoek behoort NIET
De technische en organisatorische aspecten van Diginetwerk	Beleidskeuzen over door te voeren acties
De positionering van Diginetwerk en andere e-	Organisatorische en bestuurlijke consequenties

Tot het onderzoek behoort WEL	Tot het onderzoek behoort NIET
overheidsvoorzieningen in het OSI model en in kavel 7 (basisinfrastructuur)	van gesignaleerde risico's en witte vlekken
De risico's van Diginetwerk in relatie tot een veilige informatie-uitwisseling binnen de overheid	Juridische en financiële consequenties
De governance en het beheer van Diginetwerk	Een vergelijking van Diginetwerk met organisatiespecifieke overheidsnetwerken
De financiering van Diginetwerk	

2.4 Werkwijze

VKA heeft de volgende stappen doorlopen in het onderzoek

VOORBEREIDING

Met de begeleidingscommissie is de aanpak, de te raadplegen documentatie en stakeholders bepaald. De samenstelling van de begeleidingscommissie is opgenomen in bijlage A.

BRONSTUDIE

Documenten over de (beveiliging van) informatie-uitwisseling bij de overheid en over Diginetwerk zijn bestudeerd.
De lijst met bestudeerde documenten is opgenomen in bijlage B.

INVENTARISATIE

In overleg met de begeleidingscommissie is bepaald met welke instanties en personen een interview gehouden wordt. Een deel van de geïnterviewden heeft kennis van eisen aan veilige informatie-uitwisseling binnen de overheid, in de rol van afnemer. Een ander deel van de geïnterviewden heeft materiekennis over Diginetwerk
De lijst met gesprekspartners is opgenomen in bijlage C.

TOETSKADER

Voor de analyse van de governance, het beheer en beveiliging van Diginetwerk is een referentiekader opgesteld. Daarbij is gebruik gemaakt van reeds bestaande normenkaders aangevuld met nieuwe inzichten in het beheer en de beveiliging van infrastructuren.

ANALYSE

De uitkomsten van de bronstudie en de interviews zijn vergeleken met toetskader.

VALIDATIE

De uitkomsten van de analyse zijn besproken met materiedeskundigen op het gebied van informatie-uitwisseling en netwerken.

RAPPORTAGE

Op basis van de bespreking in de begeleidingscommissie van het concept rapport is een definitief rapport opgesteld.

2.5 Leeswijzer

In dit rapport behandelt VKA de volgende onderwerpen:

Hoofdstuk

3. Beschrijving van de beveiligingscontext van Diginetwerk.
4. De belangrijkste gebleken randvoorwaarden bij een veilige infrastructuur voor informatie-uitwisseling.
5. De wijze waarop Diginetwerk (in relatie tot andere voorzieningen) bijdraagt bij aan een veilige infrastructuur voor informatie-uitwisseling binnen de overheid.
6. De belangrijkste risico's ten aanzien van veilige informatie-uitwisseling.
7. Aanknopingspunten voor verbetering van de huidige beveiligingsinfrastructuur in termen van kosten en verantwoordelijkheden.

3 DE ONDERZOEKSCONTEXT

3.1 De beveiligingscontext van Diginetwerk

Binnen het stelsel van voorzieningen voor informatie-uitwisseling bij de overheid wordt gebruik gemaakt van o.a. Digikoppeling, Digimelding en PKI certificaten. Informatie-uitwisseling kent een aantal risico's, deze risico's zijn te mitigeren door het treffen van een samenhangend pakket van (beveiligings-) maatregelen in de techniek, in de organisatie en in de fysieke omgeving. Door de juiste keuze te maken in de te selecteren maatregelen wordt de beveiliging van alle componenten in een keten op een gewenst beveiligingsniveau gebracht waarbij de kosten acceptabel zijn en de restrisico's te beheersen zijn.

Voorzieningen zoals Diginetwerk, Digikoppeling en PKI certificaten bieden de mogelijkheid om informatie uitwisseling op verschillende wijze te beveiligingen, op netwerkniveau (transportlaag), op het niveau van uitwisseling van berichten (logistieke laag) of op het niveau van de inhoud zelf ("inhoud laag"). De keuze voor de gewenste soort beveiliging is afhankelijk van de eisen en wensen van de stakeholders. Zij bepalen vanuit hun verantwoordelijkheid het beveiligingsniveau en de risico's die zij wensen te aanvaarden. Op basis van deze eisen dient voor de gehele keten bekeken te worden waar de maatregelen op de meest effectieve, efficiënt (w.o. kosten/ baten) getroffen kunnen worden.

Op dit moment bestaat geen samenhangend beeld van de beveiligingseisen, risico's en randvoorwaarden die gesteld worden aan Diginetwerk, de aanpalende netwerken en de voorzieningen die zich daarin bevinden, bezien vanuit de belangrijkste stakeholders, zoals de Belastingdienst, RWS, SUWI-partners, gemeenten (Gemnet), RINIS en de Haagse Ring. Diginetwerk vormt een belangrijke verbindende schakel in de informatie-uitwisseling binnen de overheid. Het legt een (fysieke) verbinding tussen verschillende netwerken van publieke en private organisaties. Deze netwerken worden de Koppelnetwerken genoemd. Naast fysieke verbindingen met de Koppelnetwerken bestaat Diginetwerk uit een "virtueel" netwerk dat zich over de koppelnetwerken uitstrekt en waarbinnen organisaties die op Diginetwerk zijn aangesloten veilig informatie kunnen uitwisselen. De aangesloten organisaties zijn meest (semi-) overheidsorganisaties, waaronder provincies, gemeenten en waterschappen, maar ook op de Koppelnetwerken aangesloten private organisaties die voor uitvoering van publieke taken informatie moeten uitwisselen met genoemde (semi-)overheidsorganisaties.
Koppelnetwerken verbonden met Diginetwerk zijn Suwinet, Haagse Ring en, Gemnet.

Diginetwerk is een besloten netwerk en maakt het, volgens de beschrijving van de dienst Diginetwerk, mogelijk om informatie uit te wisselen met classificatieniveau Departementaal Vertrouwelijk of WBP risicoklasse II. Diginetwerk kent een beschikbaarheid van >99,9%.

Door het via Diginetwerk onderling verbinden van koppelnetwerken ontstaat in wezen één virtueel netwerk voor de publieke sector, tot op zekere hoogte vergelijkbaar met Internet, alleen gericht op een beperkte doelgroep, veiliger en met een gegarandeerde beschikbaarheid en performance.

3.2 De historische context

In 2006 startte het Programma Bundeling Landelijke Netwerken (BLN). Binnen dit programma is een Programma van Uitgangspunten (PvU) opgesteld voor (de aanbesteding van) overheidsnetwerken (OT2006 data).

In 2009 is binnen GBO.Overheid de handschoen opgepakt om daadwerkelijk tot realisatie van het Koppelnet Publieke Sector te komen. Een implementatie op basis van PvU BLN heeft geleid tot de ontwikkeling van het BasisKoppelnetwerk (BKN).

De afgelopen jaren is het gebruik en het beheer van Diginetwerk geleidelijk uitgebouwd.

4 RANDVOORWAARDEN BIJ VEILIGE INFORMATIE-UITWISSELING

In dit hoofdstuk behandelt VKA de vraag naar de randvoorwaarden die door stakeholders en beleidsmatig gesteld worden aan veilige informatie-uitwisseling binnen de overheid

4.1 Wie zijn de stakeholders rondom Diginetwerk ten behoeve van veilige informatie-uitwisseling?

De primaire doelgroep zijn organisatie binnen de overheid, de semi-overheid en particuliere organisaties met een publieke taak die op een geautomatiseerde wijze persoonsgegevens verwerken en uitwisselen en een wettelijke verplichting hebben tot het beveiligen van persoonsgegevens. Maar ook de beherende partijen van Diginetwerk en de externe leveranciers van netwerkdiensten kunnen als stakeholders beschouwd worden.
De Wet Bescherming Persoonsgegevens (WBP) biedt hiervoor een goede kapstok. De wet eist in artikel 13 dat deze organisaties passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen moeten garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, dat een passend beveiligingsniveau gerealiseerd wordt, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

4.2 Welke verwachtingen en randvoorwaarden (eisen) hebben/ stellen de stakeholders op korte, midden en lange termijn over (veilige) informatie-uitwisseling?

Stakeholders stellen eisen aan vertrouwelijkheid van informatie-uitwisseling. Regelmatig wordt WBP risicoklasse 2, verhoogd risico als beveiligingseis genoemd. In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkene);
5. alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.

Ook wordt soms WBP risicoklasse 3, hoog risico genoemd. De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt. Ook bijzondere verwerkingen van persoonsgegevens, bijvoorbeeld een DNA-databank, vallen in deze klasse.

Het CBP biedt een overzicht voor het bepalen van de risicoklasse.

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens	Financieel en / of economische persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	*Aard van de verwerking*		Conform artikel 16 WBP	
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse 0**	**Risicoklasse II**	**Risicoklasse II**
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse I**	**Risicoklasse III**	

Bij iedere risicoklasse hoort een set beveiligingsmaatregelen.

De stakeholders geven aan dat beveiligingsmaatregelen van informatie-uitwisseling beginnen bij de verwerkingsprocessen van de betrokken organisaties en in de applicaties die deze processen ondersteunen. Vervolgens worden maatregelen getroffen op de koppelvlakken (zowel op het niveau van applicaties als op het niveau van bijvoorbeeld Digikoppeling). De beveiliging van het netwerk kan ook een bijdrage leveren aan de totale beveiliging. De stakeholders stellen hier geen specifieke eisen aan en zien dit als de als de eerste schil van beveiliging.
De grote afnemers benadrukken de voordelen van een besloten netwerk, vooral hoge beschikbaarheid en capaciteit.

Voor wat betreft de toekomstige invulling van de beveiligingsmaatregelen ziet VKA verschillende beelden. Sommige stakeholders zien de beveiligingsmaatregelen verschuiven naar de aangesloten systemen, waarbij overheidsorganisaties direct op Internet zijn aangesloten voor informatie-uitwisseling. Anderen wijzen erop, dat niet alle overheidsorganisaties in staat zijn hun systemen zo te beveiligen dat deze voldoende veilig direct op Internet aangesloten kunnen worden en pleiten voor het handhaven van een besloten netwerk als eerste verdediging tegen aanvallen van buitenaf.

4.3 Hoe zien de stakeholders de rol van Diginetwerk in kader van veilige informatie-uitwisseling?

Waar mogelijk maken zij gebruik van e-overheids generieke voorzieningen. Een gemeenschappelijke netwerk voorziening is goedkoper dan ieder voor zich.

De Belastingdienst hecht daarbij aan een federatief netwerk, waarbij naast een gemeenschappelijke netwerkvoorziening voor de aangesloten partijen ruimte bestaat om voor de eigen organisatie zelf een oplossing te kiezen. Dit ook om de marktwerking bij aanbesteding van netwerkdiensten niet te verstoren. Gemeenschappelijke afspraken maken op de koppelvlakken, daarachter eigen keuzes van de organisatie.

Voor het gebruik van een aantal e-overheidsvoorzieningen wordt het gebruik van Diginetwerk verplicht gesteld.
Bij de gemeenten ervaart men het koppelen via Diginetwerk soms als omslachtig (kosten, administratie en doorlooptijd). Voor gemeenten is niet altijd duidelijk en onderbouwd waarom Diginetwerk vereist is voor informatie-uitwisseling. Het Handelsregister (NHR) eist Diginetwerk terwijl burgers en bedrijven KvK gegevens via internet kunnen opvragen; gemeente sluiten via Digikoppeling (eBMS) over internet aan op MijnOverheid; uitvoeringsorganisaties doen dit via Diginetwerk; eFactureren vereist Diginetwerk terwijl de factuur van de leverancier via internet wordt aangeleverd.

Veel van de geïnterviewde beschouwen het als een vanzelfsprekendheid dat een besloten netwerk een hoger beveiligingsniveau biedt. Gevraagd naar de achtergrond van deze beoordeling geven zij aan dat een besloten netwerk de mogelijkheden voor een aanvaller van buitenaf om systemen op Diginetwerk aan te vallen, aanzienlijk beperkt. Met name voor partijen die minder goed in staat zijn hun beveiliging te beheersen, is dit een voordeel ten opzichte van een versleutelde verbinding over Internet. Daarnaast is de kans op verstoring door ongewenst verkeer of door aanvallen op een site kleiner.

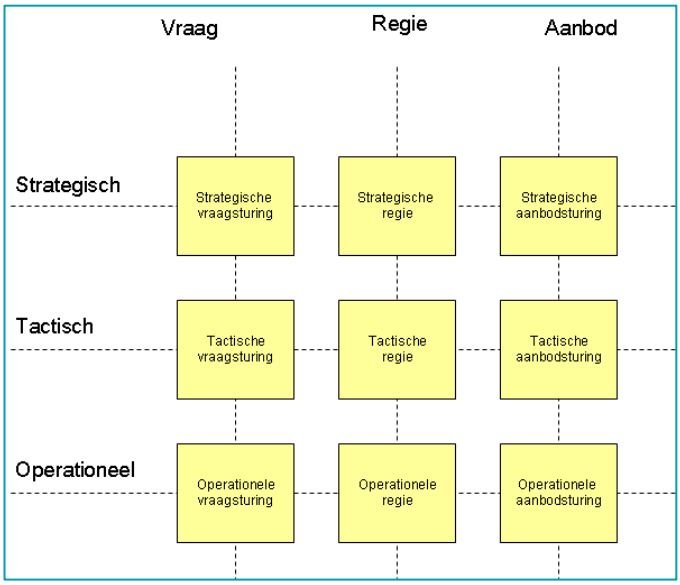
4.4 Hoe zijn het beheer, de governance en financiering rondom Diginetwerk en keten componenten ingericht?

REFERENTIEKADER VOOR GOVERNANCE EN BEHEER

Voor de kaderstellingen van governance van ICT binnen de overheid sluit VKA aan bij de omschrijving die de Algemene Rekenkamer hanteert.
"IT-governance is de gezamenlijke verantwoordelijkheid van de top van de organisatie en de toezichthouder(s) voor:
• de interne sturing van de ICT-voorziening van de organisatie;
• de interne beheersing van de ICT-voorziening van de organisatie;
• de externe verantwoording over de ICT-voorziening van de organisatie;
• het externe toezicht op de ICT-voorziening van de organisatie;
• en (bij ministeries, indien van toepassing) de aansturing van en het toezicht op de ICT-voorziening van de RWT's door het ministerie."

Op basis van dit kader kijkt VKA naar de besturing en beheersing van Diginetwerk op strategisch niveau en de wijze waarop verantwoording afgelegd wordt en toezicht wordt gehouden op Diginetwerk.

Voor de kaderstelling van beheer hanteert VKA het besturingsmodel Tactische regie op de Generieke Infrastructuur (TBGI), zoals dat door het ministerie van BZK is ontwikkeld. Dit kader sluit aan op het negenvlak voor informatiemanagement dat ontwikkeld is door de Universiteit van Amsterdam en zeer breed binnen en buiten de overheid wordt gehanteerd als analysekader voor management van de informatievoorziening.



Figuur 1 Het Amsterdams negenvlak als kader voor management van informatievoorziening

De scope van dit onderzoek betreft het beheer op strategisch, tactisch en operationeel niveau van Diginetwerk door verschillende beheerders en de relatie met de vraagsturing door de afnemers en de aanbodsturing door de externe leveranciers van Diginetwerk.
De belangrijkste begrippen uit het model worden hier toegelicht:

- Tactische regie bundelt binnen de vastgestelde strategische kaders de vraag (vraagbundeling) en beheerst het aanbod van ICT-diensten.
- Tactische vraagsturing formuleert de vraag naar ICT-diensten, zodanig dat dit de tactische verandertrajecten van de afnemers ondersteunt (vraagarticulatie).
- Strategische regie formuleert de governance en het meerjarenkader voor vraag en aanbod van ICT-diensten.
- Tactische aanbodsturing formuleert het tactische aanbod van ICT-diensten, zodanig dat het consequenties daarvan voor de dienstverlening aan de afnemers weergeeft.

Vaak is hierbij sprake van een keten van vragende en aanbiedende partijen die onderling afspraken maken over de kwaliteit van de dienstverlening. Dat kan volgens twee modellen:

1. Klant-leverancier relatie, waarbij formele (raam-) overeenkomsten worden afgesloten met daarin de rechten en plichten en eventuele sancties bij niet naleven van de overeenkomst. Dit model wordt toegepast bij uitbestedingen aan de particuliere sector.
2. Partnership relatie, waarbij samenwerkingsafspraken gemaakt worden tussen partijen over de wederzijdse dienstverlening en door middel van monitoring, overleg en evaluatie de samenwerking wordt verbeterd. Dit model wordt veelal toegepast bij samenwerking tussen overheidspartijen.

DE GOVERNANCE VAN DIGINETWERK

Betrokken partijen zijn het Ministerie van BZK, afnemers, publieke netwerkdienstverleners (Logius, BKWI, RINIS) en particuliere netwerkdienstverleners (Gemnet, KPN, BT).
Afnemers geven aan dat Diginetwerk meer als generieke infrastructuur aanbodgedreven georganiseerd zou moeten worden, met strategische regie vanuit BZK.
Logius is houder van Diginetwerk. Het eigenaarschap voor Diginetwerk wordt niet actief ingevuld. Er is geen strategisch beleids- en architectuurkader voor Diginetwerk. Ook bestaan er geen verantwoordingslijnen en vindt er geen bestuurlijk toezicht plaats op het functioneren van Diginetwerk.
Logius organiseert het collegiaal overleg met de afnemers en andere dienstaanbieders (de zogenaamde "kleine governance").
Het initiatief van BZK DGOBR om RON 2.0 vorm te geven in het licht van de aanbesteding ON 2013 wordt door de afnemers gewaardeerd. Als aandachtspunt daarbij wordt genoemd dat ON2013 zich lijkt te beperken tot het Rijk, terwijl in de huidige praktijk veel semi-overheidsorganisaties en andere overheden gebruik maken van Diginetwerk.

BEHEER

Omdat Diginetwerk zelf niet één fysiek netwerk is maar een basiskoppelnet (BKN) dat meerdere koppelnetwerken onderling verbindt, is niet sprake van één beheerder die volledig op Diginetwerk toeziet. Logius voert het tactisch beheer van Diginetwerk, maar is voor de uitvoering daarvan afhankelijk van de beheerders van de koppelnetwerken. Elk van de koppelnetwerken heeft een eigen operationele, tactische en strategische beheerder.

Bij Diginetwerk zijn de volgende beheerpartijen betrokken.

Koppelnetwerk	**Tactisch beheerder**	**Netwerk leverancier**
Haagse Ring OSB VPN OT Wolk	Logius	IVent BT-Nederland en KPN
SUWInet	BKWI	KPN
Gemnet	Gemnet	KPN

Het tactisch beheer van het BasisKoppelNetwerk (BKN), dat de koppelnetwerken verbindt, ligt bij Logius. Het operationeel beheer van BKN wordt uitgevoerd door BKWI. De leverancier van BKN is KPN.
BKWI maakt voor het operationele beheer gebruik van een onderaannemers (externe partij, Quanza Engineering B.V.).

Volgens de "Samenwerkingsovereenkomst Basiskoppelnetwerk Diginetwerk", versie 1.0, 10 september 2010 (overeenkomst tussen Logius en BKWI), is Logius verantwoordelijk voor de uitvoering van de volgende taken: onderhouden van contacten en afspraken met de belangrijkste stakeholders van Diginetwerk; het ontwerp en de planning van Diginetwerk; en het beleid met betrekking tot netwerkbeveiliging. Uitvoering van overige activiteiten, zoals bijvoorbeeld Service

Delivery en Service Support taken en het beheer over de uitgifte van IP-nummers, ligt bij BKWI. Voor een deel van deze BKWI taken ligt de eindverantwoordelijkheid bij Logius.

De koppelnetwerkbeheerders sluiten afnemers aan. Diginetwerk is een additionele netwerkdienst die een koppelnetwerkbeheerder levert in aanvulling op de bestaande dienstverlening aan zijn afnemer.

Er zijn aansluitvoorwaarden voor beheerders van de Koppelnetwerken die namens Logius de toegang tot de Diginetwerkdienst aanbiedt aan afnemers. Hierin is opgenomen dat beveiligingseisen gesteld kunnen worden aan afnemers (w.o. scheiding van internet). Zo stelt Haagse ring de eis dat afnemers jaarlijks een mededeling overleggen, af te geven door de departementale accountantsdienst of een onafhankelijke derde (TPM), waaruit blijkt dat het beheer en de beveiliging van de eigen netwerkinfrastructuur adequaat zijn en derhalve geen bedreiging vormen voor de overige Haagse Ring partijen. De afnemers, bijvoorbeeld gemeenten, beschikken over eigen (interne) bedrijfsnetwerken die weer (fysiek) worden aangesloten op de koppelnetwerken. Het beheer over deze bedrijfsnetwerken, en daarmee het toezien op de beveiliging hiervan, is een verantwoordelijkheid van de aangesloten organisatie.

Logius geeft aan voor haar BKN dienstverlening een Servicelevel Overeenkomst te hebben met de koppelnetbeheerders. Dit is verder niet onderzocht.

Binnen SUWInet worden beveiligingsaudits uitgevoerd bij aangesloten partijen. RINIS beschouwt Diginetwerk als een onveilige externe omgeving en hanteert eigen beveiligingsmaatregelen (VPN PKI Overheid).
Gemnet kent geen genormeerd beveiligingsniveau (in de zin van WBP klasse 3, 2 of departementaal vertrouwelijk), maar hanteert wel het principe van een "besloten" netwerk en stelt aansluitvoorwaarden aan haar klanten.

FINANCIERING

- De kosten van Logius voor Diginetwerk worden deels op basis van een businesscase gedragen door een aantal stakeholders. De kosten voor de generieke voorzieningen worden omgeslagen over andere Logius producten die gebruik maken van Diginetwerk. BZK financiert Diginetwerk niet.
- BKWI wordt centraal gefinancierd door SZW. BKWI betaalt de verbindingen naar de centrale omgeving (rekencentra APG) en de verbindingen naar GemNet en het Basiskoppelnet van DigiNetwerk. De via de infrastructuur aangesloten partijen (SVB, UWV, OCWDUO en Wigo4it) betalen voor hun eigen verbindingen. Alle overige bronnen en afnemers op/van Suwinet worden via DigiNetwerk door de Haagse Ring of GemNet ontsloten. Zij betalen uitsluitend voor die aansluiting.
- Deelnemers aan RINIS betalen een abonnement en een tarief per afgeleverd bericht (op basis van BSN) of per omvang van het bericht, als BSN niet bekend is. Tarieven worden door de RvT vastgesteld. De projs van het tarief neemt af bij grote afname. Daarnaast is er een vast tarief voor koppeling van RINISnet aan andere netwerken, zoals sTesta en Diginetwerk.

- Gemeenten betalen voor dienstverlening van Gemnet. Logius geeft aan een contractrelatie te hebben met Gemnet voor de additionele dienst van Gemnet 'Aansluiting Op Diginetwerk' (AOD. Gemeenten betalen een jaarlijkse bijdrage voor het aansluiten op AOD).

4.5 Welke normenkaders zijn van toepassing voor Informatiebeveiliging en voor informatie-uitwisseling?

Voor alle aangesloten deelnemers geldt de algemene wet- en regelgeving, waaruit de belangrijkste zijn:

- Wet Bescherming Persoonsgegevens (WBP)
- Beveiliging van persoonsgegevens (Achtergrondstudies & Verkenningen nr 23 van de Registratiekamer, nu het College Bescherming Persoonsgegevens, ter nadere invulling van de WBP)

Voor organisaties binnen de Rijksoverheid zijn de algemene normenkaders voor informatiebeveiliging binnen de Rijksoverheid van toepassing. Deze zijn in wisselende mate ook geldig voor zelfstandige uitvoeringsorganisaties:

- Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI 2012)

Deze wetten, regels en normen stellen eisen aan de wijze waarop de organisatie omgaat met informatie. De eisen richten zich in het algemeen niet op de te gebruiken netwerken. In het algemeen wordt gesteld dat passende maatregelen genomen moeten worden die aftappen en ongeautoriseerd modificeren van gegevens tegengaan en dat passende maatregelen genomen moeten worden om de continuïteit van de netwerkdiensten te borgen. Welke maatregelen genomen moeten worden, hangt af van de specifieke waarde van de gegevens en de risico's eromheen. Specifieke maatregelen op netwerkniveau worden niet genoemd, anders dan dat gegevens die over niet-vertrouwde netwerken worden getransporteerd, moeten worden versleuteld als ze niet openbaar zijn.

Voor een aantal deelnemers geldt sectorspecifieke wet- en regelgeving:

- SUWI wet
- GBA wet
- Belastingwetgeving
- Sectorspecifieke regels

De wetten en regels zijn top-down opgezet. Er worden eisen gesteld aan de beveiliging, waaraan met verschillende sets van maatregelen invulling gegeven kan worden. In de wetten en regels ligt niet vast welk deel van de eisen wordt ingevuld met maatregelen in de sfeer van het netwerk. Met andere woorden: welke maatregelen genomen worden op het niveau van het netwerk en maatregelen in andere delen van de informatieverwerking is een afweging van de betrokken partijen.

4.6 Welke relevante documentatie worden als uitgangspunt genomen?

Voor dit onderzoek zijn als uitgangspunt voor de eisen aan informatiebeveiliging de volgende documenten uit het algemene normenkaders voor informatiebeveiliging genomen:

- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2005)
- NORA 3.0, specifiek het Informatiebeveiligingskatern
- NORA 2.0, specifiek het hoofdstuk Beveiliging en Privacy
- Baseline Informatiebeveiliging Rijksdienst (BIR)
- Achtergrondstudies en verkenningen (AV) 23 van de Registratiekamer (nu CBP)

5 BIJDRAGE VAN DIGINETWERK AAN VEILIGE INFORMATIE-UITWISSELING

5.1 Wat is het doel van Diginetwerk?

De doelstelling van Diginetwerk is terug te vinden in de Diginetwerk architectuur beschrijving:

> Het doel van Diginetwerk is om een efficiënte en effectieve standaardoplossing te bieden op het gebied van connectiviteit voor een omschreven toepassingsgebied.
> Diginetwerk levert een situatie waarin elke organisatie binnen het publieke domein elke andere organisatie daarbinnen kan bereiken, op eenvoudige en gestandaardiseerde wijze via geharmoniseerde en in samenhang gekoppelde netwerken, die optimaal voorzien in de functionele connectiviteitsbehoefte.

> Diginetwerk is bedoeld voor uitwisselingen tussen overheidsorganisaties waarvoor een hoog niveau van betrouwbaarheid/beveiliging vereist is.

In de kern is Diginetwerk (status 2012):

a. Een fysiek netwerkknooppunt (het “BKN", BasisKoppelNetwerk), bestaande uit een tweetal koppelpunten (2 locaties met netwerkapparatuur) waarop een (beperkt) aantal koppelnetwerken is aangesloten ten behoeve van onderlinge informatieuitwisseling.
b. Een verzameling afspraken tussen Diginetwerk en de beheerders van koppelnetwerken over de informatie-uitwisseling tussen (overheids-) organisaties. Deze afspraken hebben betrekking op de voorwaarden waaronder deze informatie-uitwisseling plaatsvindt. (“besloten”, beschikbaarheid, informatiebeveiliging, netwerkadressering, informatiefiltering).

Het geheel van BKN, de koppelnetwerken en de verzameling afspraken zorgt voor één "virtueel" netwerk waarop overheidsorganisaties kunnen worden aangesloten zonder dat de complexiteit van de onderliggende infrastructuur (koppelnetwerken, BKN) voor deze organisaties zichtbaar is.

Diginetwerk heeft een federatief karakter. De verantwoordelijkheid voor het implementeren en controleren van de gemaakte afspraken is een verantwoordelijkheid van elk van de aangesloten koppelnetwerken en de daarop aangesloten organisaties. Diginetwerk, koppelnetwerken en aangesloten organisaties vormen één “trusted domein”. Er vindt geen centraal toezicht op de naleving plaats.

5.2 Wie zijn aangesloten op Diginetwerk?

De beheerder van Diginetwerk (Logius) heeft geen directe contractuele relatie met de organisaties die van Diginetwerk gebruik maken. De beheerders van de koppelnetwerken zijn verantwoordelijk

voor het aansluiten van organisaties op Diginetwerk (voor zowel de fysieke aansluiting als de "logische" aansluiting op Diginetwerk). Logius heeft met de beheerders afspraken gemaakt over de blokken IP adressen die voor de koppeling met Diginetwerk gebruikt kunnen worden. IP Adressen binnen deze blokken kunnen door de koppelnetwerkbeheerders worden gebruikt om (nieuwe) organisaties te verbinden met Diginetwerk, zonder dat hiervoor handelingen van de kant van Logius nodig zijn. In technische zin heeft Logius daarmee geen inzicht in welke organisaties door de koppelnetwerkbeheerders op Diginetwerk worden aangesloten. De verantwoordelijkheid voor het aansluiten op Diginetwerk en het bijhouden van een overzicht met aangesloten organisaties is daarmee een verantwoordelijkheid voor de koppelnetwerkbeheerder.

Logius heeft de aansluitvoorwaarden op Diginetwerk vastgelegd in het document "Aansluitvoorwaarden Diginetwerk (16 december 2010, versie 1.71)". De bepalingen hierin betreffen voorwaarden waaronder koppelnetwerkbeheerders ("Aanbieders" genoemd) Diginetwerk aanbieden. De organisaties die door de Aanbieder op het Diginetwerk worden aangesloten worden in deze aansluitvoorwaarden Afnemers genoemd. De volgende definitie wordt gehanteerd voor een Afnemer:

> *1.3 Afnemer:*
> *Een overheidsorganisatie, publiekrechtelijke of een privaatrechtelijke organisatie, een college of een persoon met een publieke taak of bevoegdheid die voor de uitoefening van die publieke taak om reden van performance, beveiliging inclusief beschikbaarheid geen gebruik kan maken van een openbare netwerk (internet). Een overheidsorganisatie of publiekrechtelijke organisatie bepaald of de performance of beveiligingsreden van toepassing zijn.*

	Koppelnetwerk	Op Diginetwerk aangesloten organisaties ("Logische koppeling")
Diginetwerk (BKN)	Suwinet	▪ Suwinet-partners
	Haagsche ring (OSB-VPN)	▪ Departementen
	Gemnet	▪ Gemeenten ▪ GBA ▪ Externe partijen (bijv. KvK)
	RINISnet (via Haagse ring / Rijksconnect)	▪ SVB, Belastingdienst
	OT-Wolk	▪ Gemeenten, Uitvoeringsorganisaties , …

Overzicht van organisaties aangesloten op Diginetwerk. Uit "Diginetwerk totaal"

5.3 Wat is de visie en wat zijn de normen van NORA voor veilige informatie-uitwisseling binnen de overheid

Bij de opzet van Diginetwerk is uitgegaan van NORA 2.0. Over de communicatie tussen overheidsorganisaties zegt NORA 2.0, principe 7.3.1., het volgende:

7.3.1 	Eoverheids principe	P17 P19	***Communicatie tussen overheidsorganisaties verloopt via besloten, separate netwerken of door middel van een virtual private network verbinding via netwerken van particuliere bedrijven.***
Overheid-naar-overheid communicatie verloopt bij voorkeur via private netwerken met een besloten karakter. Alternatief is het realiseren van een virtueel privaat netwerk over publieke netwerken. Het betreft in beide gevallen beslotenheid. Slechts overheidsinstanties hebben toegang tot het netwerk. Verkeer tussen overheidsinstanties kan hierdoor niet snel in handen van onbevoegde derden vallen. Bovendien is de kans op aanvallen van binnenuit in een dergelijk besloten netwerk wezenlijk kleiner dan op een openbaar netwerk.			

Bij de uitwerking van dit principe is uitgegaan van de volgende voor Diginetwerk relevante Principes. Deze principes zijn één op één overgenomen uit het document "Diginetwerk Architectuur, versie 0.99, 15 november 2010".

AP 5	**Gebruik standaard oplossingen**	***De dienst maakt gebruik van standaard oplossingen***
		Afgeleid Standaard: “Afnemers ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen.”
AP 7	**Gebruik open standaarden**	Statement ***De dienst maakt gebruik van open standaarden***
AP 27	**Afspraken vastgelegd**	Statement ***Dienstverlener en afnemer hebben afspraken vastgelegd over de levering van de Dienst***
AP 28	**Consequenties van normafwijking**	Statement ***Wanneer wordt afgeweken van afspraken en standaarden draagt de dienstverlener zelf de consequenties daarvan.***
		Implicaties: Alle partijen moeten zich aanpassen c.q. rekening houden met de gevestigde communicatienormen en -standaarden. Partijen die zich niet conformeren, lopen de kans uitgesloten te worden om een bijdrage te leveren aan de dienstverlening.
AP 29	**Verantwoording dienstlevering mogelijk**	Statement ***De wijze waarop een dienst geleverd is, kan worden verantwoord***
AP 32	**Baseline kwaliteit diensten**	Statement ***De dienst voldoet aan de kwaliteitsbaseline***

		Afgeleid • Standaard: “Overeenkomstige aspecten van dienstverlening krijgen op overeenkomstige wijze vorm door gebruik te maken van generieke oplossingen die breed worden toegepast”. • Betrouwbaar: “De beschikbaarheid en de kwaliteit van diensten voldoen aan vooraf bepaalde normen”.
AP 33	**Verantwoording kwaliteit**	Statement ***De dienstverlener legt verantwoording af over de besturing van de kwaliteit van de dienst***
		Afgeleid • Transparant: “Afnemer hebben inzage in voor hen relevante informatie” • Betrouwbaar: “de beschikbaarheid en de kwaliteit van diensten voldoen aan vooraf bepaalde normen”.
AP 34	**Continuïteit van de dienst**	Statement ***De levering van de dienst aan de afnemer is continu gewaarborgd.***
		Afgeleid • Betrouwbaar: “De beschikbaarheid en de kwaliteit van diensten voldoen aan vooraf bepaalde normen.”
AP 37	**Informatiebeveiliging door filtering en zonering.**	Statement ***De betrokken faciliteiten zijn met behulp van filters gescheiden in zones***

Met betrekking tot principe AP37, Informatiebeveiliging door filtering en zonering, is meer informatie terug te vinden in "NORA Normen Informatiebeveiliging ICT-voorzieningen". Zie hiervoor bijlage D. Niet voor alle principes is even duidelijk gemaakt wat de consequenties zijn voor de inrichting van de transportlaag, of hoe het principe is vertaald naar maatregelen voor Diginetwerk.

NORA 3.0 geeft weinig concrete aanknopingspunten voor informatiebeveiliging. NORA 3.0 definieert principes voor de samenwerking en dienstverlening geldend voor de e-Overheid.

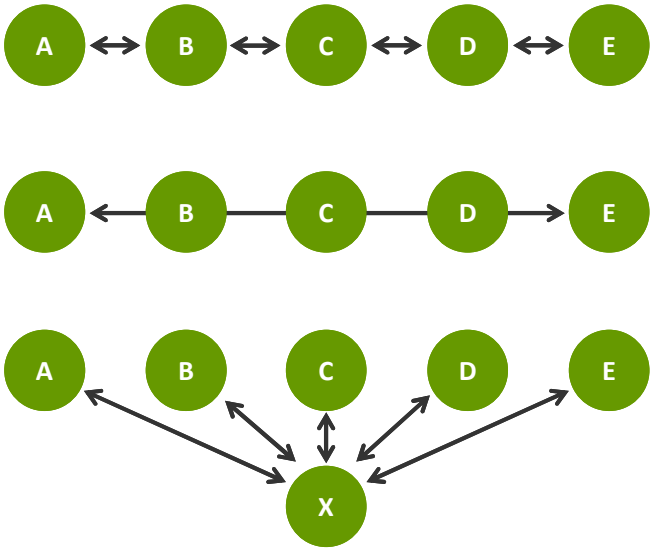
Verder kent NORA 3.0 een Dossier Informatiebeveiliging, waarin de verschillende (technische) functies voor informatiebeveiliging worden beschreven en verwijst het naar de BIR (Baseline Informatiebeveiliging Rijksdienst) en de Code voor informatiebeveiliging. In de BIR wordt gesteld dat gegevens die worden getransporteerd over onvertrouwde netwerken, moeten zijn versleuteld. Het principe van zonering wordt verder uitgewerkt in hoofdstuk 5 van het Dossier Informatiebeveiliging van de NORA. Hier wordt aangegeven dat bij datatransport over een onvertrouwd netwerk encryptie moet worden toegepast. Dit komt ook terug in de recentelijk gepubliceerde security patronen van het Platform voor InformatieBeveiliging (PvIB), dat een verdere uitwerking geeft op het NORA dossier Informatiebeveiliging en best practices op het gebied van informatiebeveiliging beschrijft.

5.4 Op welke wijze kan men veilige informatie uitwisselen in ketens?

Er zijn drie modellen voor veilige informatie-uitwisseling tussen partijen in de keten:

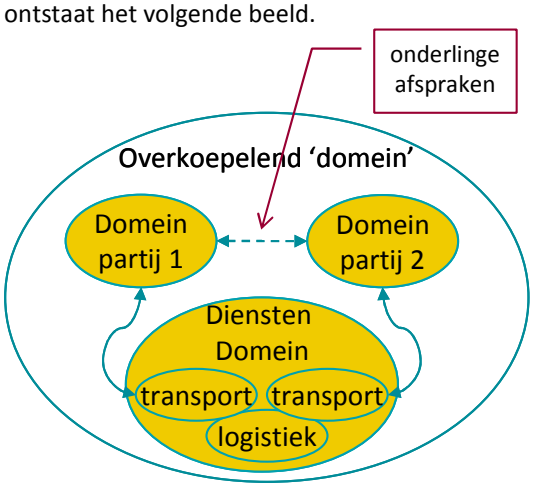
1. Elke partij is verantwoordelijk voor de informatiebeveiliging en maakt afspraken met de direct gekoppelde partners in de keten.
2. Er worden afspraken gemaakt over de informatiebeveiliging met alle betrokken ketenpartners; de implementatie hiervan is een verantwoordelijkheid van elke partij zelf.
3. Informatie-uitwisseling vindt plaats via één trusted partij. Elke partij maakt afspraken met deze trusted partij.

Een en ander is geïllustreerd in onderstaande figuur.



Figuur 2 Verschillende modellen voor informatie-uitwisseling in ketens

Als uitgegaan wordt van informatie-uitwisseling tussen twee partijen (dus niet de hele keten), dan ontstaat het volgende beeld.

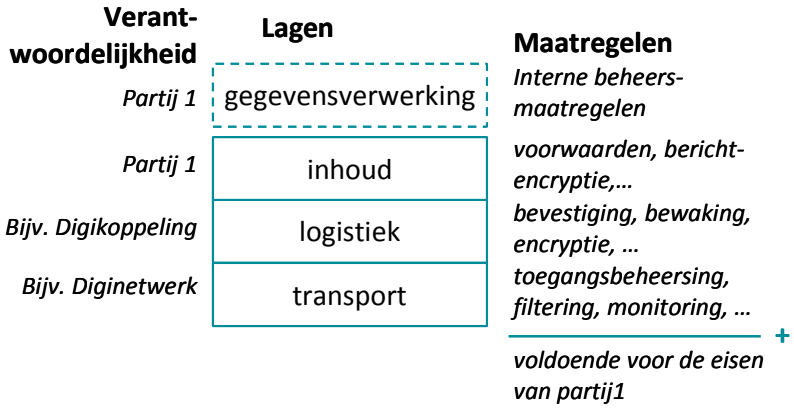


Figuur 3 Beveiligingseisen in domeinen

5.5 Wat is een veilige infrastructuur?

Voor elk van die partijen geldt in het algemeen dat deze maar gedeeltelijk vertrouwen op de maatregelen die genomen zijn in de infrastructuur. Elke partij zal ook maatregelen nemen in het eigen domein. Het totaal aan maatregelen bepaalt, of de gegevensverwerking van die partij voldoet aan de eisen die eraan gesteld worden.

De functies voor informatie-uitwisseling zijn te verdelen in een drietal “lagen”. De onderste laag, transport, omvat het datanetwerk dat wordt gebruikt. In deze laag worden alleen pakketjes data vervoerd, los van indeling, timing, of betekenis. De tweede laag “logistiek” omvat de functies die nodig zijn om de gegevens in voor de applicatie handzame eenheden, bijv. bestanden, berichten, webpagina’s, over te brengen. Deze laag bevat tevens functies om te bewaken dat gegevens inderdaad zijn overgedragen en bewaakt de timing. De derde "inhoud" laag bevat functionaliteit om de inhoud van de berichten te borgen. Hier worden de bestanden of berichten samengesteld en gelezen. In deze laag horen afspraken thuis over betekenis van gegevens en structuur van berichten. In deze laag kan ook worden geborgd dat de gegevens conform gemaakte afspraken worden uitgewisseld.



Figuur 4 Beveiligingseisen in lagen

Door de functie van deze lagen toe te wijzen aan afzonderlijke systemen en services en vervolgens te bepalen welke partijen verantwoordelijk zijn voor de diensten van de laag worden de lagen in het domein van een van de partijen uit Figuur 3 ondergebracht.

Omdat elke partij ook in het eigen domein maatregelen neemt en maatregelen over verschillende lagen van de infrastructuur worden verdeeld, zal het niet zo zijn dat alle partijen hun eisen onverminderd opleggen aan de infrastructuur. De eisen die partijen stellen aan het beveiligingsniveau en de te nemen maatregelen van de infrastructuur, zullen tot stand komen op basis van risicoanalyses en onderling overleg. Op basis hiervan kan vervolgens een onderbouwde keuze gemaakt worden voor invulling van de transportlaag. Op hoofdlijnen zijn de volgende mogelijkheden te onderscheiden:

1. Elke organisatie beslist over zijn eigen transportlaag, en de afzonderlijke infrastructuren worden waar nodig onderling gekoppeld;

2. Er wordt één besloten infrastructuur gerealiseerd (fysieke of virtueel, gebruikmakend van besloten fysieke netwerken) waarop alle partijen zijn aangesloten;
3. Gebruik van (beveiligde) internetverbindingen.

Een goede afweging tussen deze opties voor de infrastructuur kan pas worden gemaakt nadat de risicoanalyses over de drie lagen (inhoud, logistiek en transport) zijn opgesteld.

5.6 Welke componenten vormen de keten voor informatie-uitwisseling binnen de overheid (Digikoppeling, Digipoort, etc)?

Informatie-uitwisseling wordt in dit rapport ingedeeld in drie lagen. Deze indeling wordt ook gehanteerd in het architectuurdocument van Diginetwerk. Elke laag bevat functies waardoor informatie kan worden uitgewisseld. In de praktijk zijn deze functies niet altijd één op één te vertalen naar componenten. Sommige componenten bevatten meerdere functies. Dit kunnen zelfs functies zijn die zich in het model op een andere laag bevinden. Uit oogpunt van eenvoud worden de componenten in deze paragraaf beschreven per laag.

INHOUD

De inhoud laag betreft de organisatorische en inhoudelijke afstemming. Om informatie-uitwisseling te realiseren moeten organisaties afspraken maken over de inhoud: betekenis en voorgenomen gebruik (semantiek) en de manier waarop de gegevens worden gecodeerd en vertaald (syntax van de gegevens en structuur in berichten of bestanden). Alle bij de uitwisseling betrokken organisaties moeten die afspraken implementeren in hun applicaties.

Binnen de e-overheid wordt veel gebruik gemaakt van ebXML en StUF (standaaruitwisselingsformaat) als standaarden voor de berichtstructuur. Ook wordt gebruik gemaakt van XBRL (XML business reporting), met name door de Belastingdienst.

Het is mogelijk om op berichtniveau overeen te komen dat encryptie van (delen van) berichten plaatsvindt om de inhoud te beschermen. In plaats daarvan kan encryptie ook plaatsvinden op de logistiek laag.

LOGISTIEK

Applicaties en gebruikers hoeven (gelukkig) niet het IP-adres te weten van de andere partij waarmee wordt gecommuniceerd. Het IP-adres is het "straat, huisnummer, postcode, woonplaats" adres dat binnen communicatienetwerken gebruikt wordt om informatie te transporteren van computer A naar computer B. In plaats van dit adres kan worden volstaan met de logische naam van een toepassing, bijvoorbeeld www.overheid.nl. De aanbieder van netwerkdiensten zorgt ervoor dat dit logische adres wordt vertaald naar een IP-adres zodat de transportlaag weet waar het pakket met informatie naartoe gestuurd moet worden. Deze functie wordt vervuld door het Domain Name System (DNS). Diginetwerk zelf kent geen DNS functie, maar koppelt wel de Gemnet DNS en Rijks-DNS.

PKI is de infrastructuur voor vertrouwde uitwisseling van publieke sleutels voor de beveiliging van gegevens en communicatie. PKI vindt toepassing op verschillende manieren:

- Voor het opzetten van een beveiligde sessie door middel van TLS (SSL). Daarbij worden de server en eventueel de client geauthenticeerd en de gegevens worden versleuteld tijdens de overdracht.
- Voor authenticatie en ondertekening van berichten. Dit kan gebeuren op het niveau van de XML berichten zelf (XADES of WS security) of door middel van generieke beveiligde enveloppen (CMS of CADES).
- Voor encryptie van berichten. Dit kan gebeuren op het niveau van XML/SOAP berichten (WS encryption) of door middel van generieke beveiligde enveloppen (CMS).

Digikoppeling is een overheidsbrede servicebus van de Nederlandse overheid. Binnen Digikoppeling worden de ebMS en WUS standaarden gebruikt voor het uitwisselen van meldingen resp. automatisch bevragen van systemen. WSRM is voorgesteld als alternatieve standaard maar is nog niet geaccepteerd. De Digikoppeling adapter biedt faciliteiten om berichten van intern formaat om te zetten naar ebMS en WUS en omgekeerd en om de ebMS overeenkomsten voor informatie-uitwisseling te beheren. Dit moet per berichttype of per uitwisseling worden ingeregeld. Daarnaast bestuurt de adapter de logistiek van de uitgewisselde berichten.

TRANSPORT (DIGINETWERK)

In de transport laag zijn voor de uitwisseling van informatie de volgende componenten aanwezig:

- Elektronische schakelapparatuur zoals switches en routers. Deze zorgen voor versturen, routeren en ontvangen van pakketten met informatie door het netwerk.
- Elektronische apparatuur voor inspectie en filtering van informatie ("firewall"). Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.
- Bekabeling. De elektronische netwerkapparatuur wordt onderling verbonden met kabels, Tegenwoordig zijn dit, zeker bij het verbinden van apparatuur op geografisch gescheiden locaties, vaak glasvezelkabels. Hierbij kan gebruik gemaakt worden van speciale optische apparatuur (zoals DWDM-multiplexers) om de routers op een glasvezel aan te sluiten zodat optimaal van de glasvezel capaciteit gebruik gemaakt wordt.
- Housing. De elektronische (en eventueel optische) apparatuur staat in het algemeen in speciale daarvoor ingerichte ruimtes. Dit kan zijn bij de beheerder van het netwerk of bij een externe partij.

5.7 Wat is de relatie tussen Diginetwerk en de overige e-overheidsvoorzieningen in de keten voor informatie-uitwisseling? Hoe zijn deze gepositioneerd in de OSI-lagen?

Het antwoord op deze vraag is opgenomen in 5.6. De daar gemaakte indeling in drie lagen is als volgt op het OSI lagenmodel af te beelden:

- Inhoud: OSI-lagen 6 en 7;
- Logistiek: OSI-lagen 4 en 5;

- Transport: OSI-lagen 1-3.

5.8 Welke informatiebeveiligingsmaatregelen zijn er nu getroffen in Diginetwerk?

De informatiebeveiligingsmaatregelen zijn onder te verdelen in een drietal categorieën:

1. Maatregelen die Logius zelf treft op het niveau van BKN;
   - Verantwoordelijkheid voor de implementatie: Logius
2. Maatregelen die voortkomen uit afspraken tussen Logius en de beheerder van het koppelnetwerk en die van toepassing zijn op het koppelnetwerk.
   - Verantwoordelijkheid voor de implementatie: Beheerder koppelnetwerk
3. Maatregelen die voortkomen uit afspraken tussen de beheerder van het koppelnetwerk en de beheerder van het bedrijfsnetwerk van de organisatie die op Diginetwerk is aangesloten. Deze categorie maatregelen hebben betrekking op het bedrijfsnetwerk. Logius levert input voor de overeenkomst tussen koppelnetwerkbeheerder en beheerder bedrijfsnetwerk in de vorm van Aansluitvoorwaarden Diginetwerk.
   - Verantwoordelijkheid voor de implementatie: Beheerder bedrijfsnetwerk

Uit bovenstaande volgt dat de informatiebeveiligingsmaatregelen Diginetwerk zich uitstrekken over drie netwerken: Diginetwerk, Koppelnetwerk(en) en Bedrijfsnetwerk(en).

Op grond van de gevoerde gesprekken, de beschrijving Diginetwerk architectuur en de aansluitvoorwaarden Diginetwerk is VKA gekomen tot het volgende overzicht van (technische) maatregelen:

		Maatregel	Verantwoordelijkheid
Beschikbaarheid	B1	Redundantie in netwerkcomponenten, verbindingen en aansluitingen van koppelnetwerken.	Beheerder(s) Diginetwerk & Koppelnetwerk Optioneel: beheerders bedrijfsnetwerk
	B2	Procedures en tools om in geval van storingen de oorzaak snel te achterhalen.	Gezamenlijke verantwoordelijkheid, vnl. beheerders Diginetwerk en Koppelnetwerken.
Exclusiviteit	E1	Dienst is alleen beschikbaar voor organisaties met toegang tot Diginetwerk.	Beheerder(s) Diginetwerk & Koppelnetwerken
	E2	Alleen bekende organisaties wordt toegang verleent tot Diginetwerk (“besloten” netwerk).	Beheerders Koppelnetwerken
	E3	Alleen verkeertype HTTP(s), poort 443, doorgelaten.	Beheerder Diginetwerk
	E4	Diginetwerk is gescheiden van het Internet.	Beheerders Koppelnetwerken & Bedrijfsnetwerken
Integriteit	I1	Zie E4.	
	I2	Bescherming tegen “ongewenst verkeer” (hackers, virussen, spyware, spam).	Beheerders Bedrijfsnetwerken

Naast genoemde technische maatregelen zijn er organisatorische en procesmatige afspraken die bijdragen aan de informatiebeveiliging Diginetwerk. Te noemen valt:

- De mogelijkheid van de koppelnetwerkbeheerder om de aansluiting van afnemers op Diginetwerk tijdelijk op te schorten indien er sprake is van een beveiligingsincident.

- Een afspraak tussen koppelnetwerkbeheerder en beheerder bedrijfsnetwerk met betrekking tot geheimhouding van informatie.
- De afspraak dat een organisatie die van Diginetwerk gebruik maakt toestemming geeft tot een controle (door een door Logius aan te wijzen auditeur) na het veroorzaken van een beveiligingsincident.
- Een plicht voor de afnemer van de dienst Diginetwerk om beveiligingsincidenten te melden bij de koppelnetwerkbeheerder.
- Afspraken tussen Logius en de koppelnetwerkbeheerders over escalatieprocedures (technische en management escalaties).

In de huidige opzet kent Diginetwerk een beperking in het type verkeer dat via de BKN knooppunten wordt doorgelaten. Op dit moment zijn alleen beveiligde webservices (HTTPS) toegestaan. Uit gesprekken met stakeholders blijkt dat behoefte bestaat aan verruiming van deze beperking zodat ook andere typen verkeer (bijvoorbeeld e-mail) via Diginetwerk kan worden uitgewisseld. De impact van een dergelijke uitbreiding dient vooraf onderzocht te worden, niet alleen vanuit oogpunt van techniek, maar ook vanuit de risico's voor het beveiligingsniveau van Diginetwerk.

5.9 Wat zijn de ontwikkelingen (o.a. het Jericho Forum voor informatiebeveiliging) ten aanzien van infrastructurele en gegevens beveiliging voor veilige informatie-uitwisseling?

Verscheidene geïnterviewde personen hebben gesteld dat informatie-uitwisseling binnen de overheid net zo goed over openbare netwerken zoals Internet kan worden afgewikkeld, op voorwaarde dat de gegevens voldoende sterk worden versleuteld. Hierdoor zou de noodzaak voor besloten overheidsnetwerken vervallen. Dit stelt echter hoge eisen aan de beveiliging van de betreffende systemen, zowel op het vlak van technologie als beheer en security management.

Veel overheidsorganisaties gaan nog uit van beveiliging aan de rand van het netwerk. Dit veronderstelt een helder onderscheid tussen intern en extern, waarbij alle systemen op het interne bedrijfsnetwerk worden beheerd door een enkele partij en dus kunnen worden vertrouwd. De LANs op verschillende locaties zijn gekoppeld door een eigen netwerk van private verbindingen. Verkeer over het interne netwerk is in het algemeen niet versleuteld. Informatie-uitwisseling met de buitenwereld verloopt altijd via systemen voor beveiligde informatie-uitwisseling.

Dit model loopt tegen zijn grenzen aan. Het onderscheid tussen intern en extern vervaagt.

- De veiligheid van systemen, met name werkstations in het eigen netwerk, is steeds minder zeker door nieuwe dreigingen, zodat interne systemen niet zonder meer “veilig” zijn...
- Informatie-uitwisselingen tussen organisaties nemen toe in aantal en complexiteit. Tegelijk moeten organisaties aantonen dat alleen toegestane informatie-uitwisseling mogelijk is.
- Organisaties willen elkaars medewerkers toegang geven tot specifieke interne services en gegevens.

Dit heeft geleid tot de ontwikkeling van het “Jericho” model, waarbij het idee van “muren” om de ICT infrastructuur wordt verlaten. De beveiliging wordt opgezet rond de informatiesystemen en de gegevens. De beveiliging gaat niet uit van vertrouwen in de werkstations, ook al worden die goed beveiligd. Alle programmatuur die kritiek is voor de beveiliging, wordt in de centrale systemen opgenomen. Gegevens worden versleuteld over het netwerk getransporteerd. Voor de centrale login services worden zeer veilige technologieën gekozen. Er worden koppelingen gelegd tussen de centrale login services van verschillende organisaties om elkaars gebruikers te herkennen en in de eigen omgeving autorisaties toe te kennen (“federated identity” en “federated authorisation”).

Hoewel veel organisaties in het openbaar bestuur invoering van het “Jericho” model overwegen, zijn vele hier nog niet klaar voor. Men houdt daarom vast aan besloten bedrijfsnetwerken.
Een netwerk als Diginetwerk is opgezet om de systemen voor informatie-uitwisseling van organisaties binnen de overheid veilig aan elkaar te koppelen. Het bewustzijn groeit, dat deze veiligheid relatief is: als één van de organisaties een “virus” aan boord heeft, kan dit de systemen van andere organisaties aanvallen.

Een combinatie van verbeteringen in systeembeveiliging en een besloten netwerk is daarom voor velen vooralsnog de conservatieve maar veilige keuze.

6 BELANGRIJKSTE RISICO'S BIJ VEILIGE INFORMATIE-UITWISSELING

6.1 Wat zijn generieke informatiebeveiliging risico's bij informatie-uitwisseling?

Generieke dreigingen bij informatie-uitwisseling zijn:

- Aftappen van uitgewisselde gegevens;
- Onderweg wijzigen van uitgewisselde gegevens;
- Uit volgorde raken van gegevens;
- Vertraging van de informatie-uitwisseling;
- Toevoegen van berichten of bestanden aan de informatie-uitwisseling;
- Weglaten van berichten of bestanden uit de informatie-uitwisseling;
- Ongeoorloofde informatie-uitwisseling;
- Uitvallen van de informatie-uitwisseling

Daarnaast zijn er dreigingen die afkomen op de systemen die worden gebruikt voor de informatie-uitwisseling, en die ertoe kunnen leiden dat de systemen worden aangevallen, gemanipuleerd, onklaar worden gemaakt en dat er gegevens uit worden gekopieerd.

- Inbraak op systemen via andere communicatieprotocollen dan gebruikt voor de informatie-uitwisseling;
- Manipulatie van de werking door functieaanroepen en gegevens die de diensten voor informatie-uitwisseling niet correct kunnen verwerken (manipulatie binnen de communicatieprotocollen voor informatie-uitwisseling);
- Verstoring van de goede werking door aanbieden van onverwerkbare functie aanroepen of gegevens;
- Gebruik van een systeem als “springplank” naar andere systemen.

6.2 Welke risico's (w.o. informatiebeveiliging, beheer, besturing) zien de stakeholders?

Risico’s die genoemd zijn door de door de geïnterviewde personen zijn:

1. Non-compliance (leidend tot juridische en/of politieke schade).
   Hierbij merkt VKA op dat de kans op non-compliance groter wordt als de organisaties erop vertrouwen dat een gemeenschappelijke voorziening als Diginetwerk essentiële maatregelen bevat. Het zou dan moeten voldoen aan de optelling van de eisen van alle voor deelnemers geldende wet- en regelgeving. In de praktijk valt dat mee omdat de partijen sectorspecifieke wet- en regelgeving veelal in hun eigen domein implementeren en haalbare eisen aan de infrastructuur stellen.
2. Continuïteit van de (e-)overheid. Een groot aantal services van de (e-) overheid kan uitvallen als bijvoorbeeld basisregistraties niet toegankelijk zijn om basisgegevens op te halen.
3. Chaos creëren door georganiseerde misdaad of cyberterroristen. Dit risico geldt met name de politie- en justitieketens, waar tegenstanders de betreffende overheden willen afleiden of hun

functioneren willen hinderen, om ongestoord elders criminele handelingen te kunnen verrichten. Cyberterroristen kunnen uit politieke motieven of uit onvrede met overheidshandelen besluiten om verwarring te creëren.

4. Fraude door manipulatie (belasting, toeslagen). Fraude wordt veelal mogelijk gemaakt door processen te manipuleren en misbruik te maken van gebrekkige controles. Elektronische informatie-uitwisseling binnen de overheid biedt mogelijk nieuwe kansen om controles te omzeilen, frustreren of manipuleren of valse gegevens in de systemen in te brengen.
5. Aftappen van verkeer (bij netwerkprovider, etc.). Dit tast de privacy van de personen aan die deze gegevens betreffen. De steler kan de gegevens misbruiken om fraude te plegen die aan die personen en/of de overheid schade opleveren.
6. Misbruik / stelen van uitgewisselde gegevens bij een minder goed beveiligde afnemer.
7. Sluipende aantasting van de belangen van de burger door opstapeling van minieme datalekken.
   Een gevolg van het massale gebruik van elektronische informatie-uitwisseling is dat er vele kopieën van op zich onbelangrijke gegevens over personen op vele plaatsen liggen, sommige goed beveiligd, sommige minder goed. Een cybercrimineel die gegevens steelt op slecht beveiligde plaatsen en deze op de lange termijn verzamelt, kan door het combineren van gegevens over één persoon voldoende gegevens verzamelen om identiteitsfraude te plegen. Er is een levendige handel in persoonsgegevens, juist met dit doel. Om deze schade op lange termijn te voorkomen, moet de overheid en alle partijen die met persoonsgegevens omgaan, deze gegevens beter beschermen dan op het eerste oog het belang van de gegevens vereist.
8. Sluipende aantasting van de belangen van de overheid.
   Hetzelfde gevaar loopt de overheid. Spionage betreft vaak het verzamelen van zeer veel gegevens waaruit de tegenstander door analyse geheimen kan onthullen.
9. Inbreuken worden niet gedetecteerd doordat beheer niet in één hand ligt.
   Om inbreuken op de beveiliging te constateren, moet de beheerder van een netwerk of systeem dit goed monitoren en de monitoring gegevens regelmatig analyseren. In het geval van een inbraak vanaf een ander (vertrouwd?) systeem ligt de analyse moeilijker. Dit leidt tot de noodzaak, afspraken te maken over uitwisseling van monitoring gegevens bij beveiligingsincidenten.

6.3 Hoeveel risico is men bereid te nemen t.o.v. kosten/ baten/ gebruikersgemak?

De geïnterviewde personen vinden beveiliging van de informatie-uitwisseling van groot belang. Zij gaven aan geen concreet beeld te hebben hoe de afweging tussen beveiliging en gebruikersgemak te kunnen maken. Daarom kiest men er veelal voor de geldende normen en regels nauwkeurig te volgen.

6.4 Wat is de maatregelen bereidheid voor het treffen van beveiligingsmaatregelen?

De geïnterviewde personen gaven te kennen de bestaande maatregelen als een vanzelfsprekendheid te beschouwen. Men was eerder bezorgd om de gevolgen van het mogelijk verminderen van beveiligingsmaatregelen. Enkele hiervan afwijkende stellingen waren:

1. Het gebruik van een besloten netwerk is een maatregel die minder effectief wordt naarmate meer partijen van dat besloten netwerk gebruik maken.
2. Het gebruik van een besloten netwerk staat een snelle implementatie van nieuwe informatie-uitwisselingen in de weg.
3. Filteren van verkeer wordt door verschillende partijen genoemd als ineffectieve maatregel die leidt tot extra beheerinspanning.

Enkele pleitten voor het instellen van audits om partijen toe te laten tot een besloten overheidsnetwerk zoals Diginetwerk.

7 AANKNOPINGSPUNTEN VOOR VERBETERING VAN DE HUIDIGE BEVEILIGINGSINFRASTRUCTUUR

7.1 Op welke wijze kan veilige informatie-uitwisseling plaatsvinden binnen de overheid?

De essentie is dat ketenpartners die informatie uitwisselen op basis van een risicoafweging en in goed onderling overleg gezamenlijk eisen stellen aan het beveiligingsniveau van de uit te wisselen informatie en de daarbij te nemen beveiligingsmaatregelen.
In de vorige hoofdstukken heeft VKA een aantal aspecten hiervan besproken:

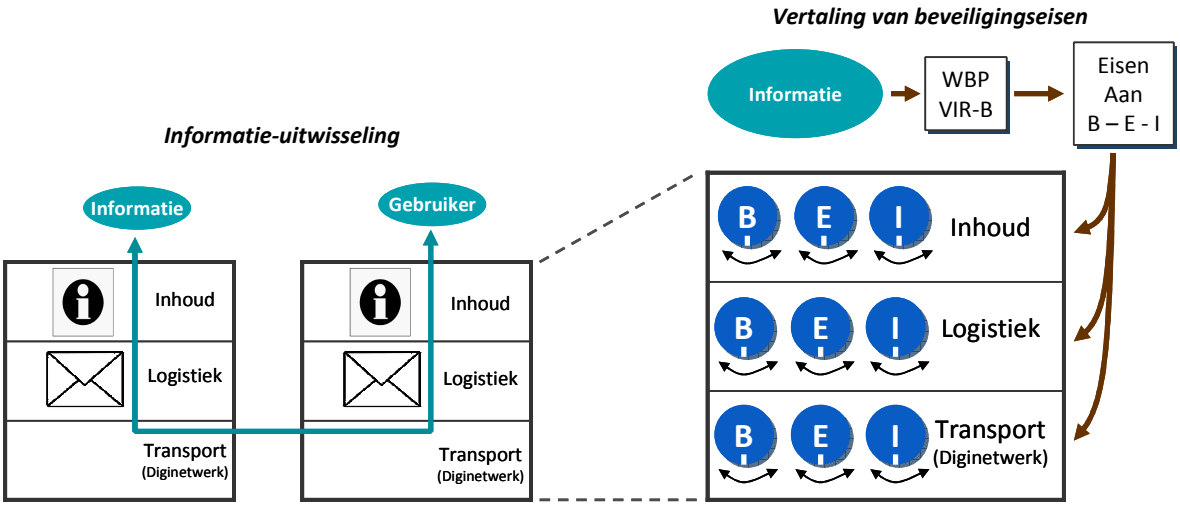
- De maatregelen om informatie te beveiligen kunnen op verschillende lagen worden genomen. Om dit inzichtelijk te maken wordt uitgegaan van drie lagen (conform NORA): inhoud, logistiek en transport (zie ook paragrafen 5.5 en 5.6).
- Voor de informatiebeveiliging gaat VKA uit van de drie kwaliteitsaspecten (B-E-I) die in de uitwerking van de AV 23 worden gehanteerd:
  1. Beschikbaarheid of continuïteit: De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Beschikbaarheid of continuïteit wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.
  2. Exclusiviteit of vertrouwelijkheid: Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.
  3. Integriteit: De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.

  Het AV 23 kader wordt naar verwachting binnenkort vervangen door de CBP richtsnoeren voor beveiliging van persoonsgegevens. Naar verwachting zal de essentie van de kaderstelling hierdoor niet wijzigen.
- De verschillende manieren waarop veilige informatie-uitwisseling in ketens kan plaatsvinden (paragraaf 5.4).
- De eisen die gesteld worden aan informatiebeveiliging in de WBP (klasse 2) en het VIR-BI (Departementaal vertrouwelijk) (zie o.a. paragraaf 4.2).

Deze paragraaf geeft een overzicht van deze punten, waardoor een totaalbeeld ontstaat over de verschillende wijzen waarop veilige informatie-uitwisseling binnen de overheid kan plaatsvinden.

Aan de uitwisseling van informatie tussen partijen worden beveiligingseisen gesteld, afhankelijk van de risicoklasse en het belang van de uit te wisselen informatie (voortkomend uit de WBP of VIR-BI).
De informatie die wordt uitgewisseld tussen partijen verloopt via de drie lagen; inhoud, logistiek en transport. Op elke laag zijn beveiligingskeuzen te maken ten aanzien van het borgen van de Beschikbaarheid, Exclusiviteit en Integriteit van de informatieverwerking. Het geheel van B-E-I maatregelen op de drie lagen vormt de beveiliging van informatie, welke moet voldoen aan de

beveiligingseisen die op de uit te wisselen informatie van toepassing zijn. Figuur 5 geeft een en ander schematisch weer. De "knoppen" in de figuur geven aan dat op elke laag maatregelen getroffen kunnen worden ten aanzien van B-E-I.



Figuur 5. Afweging van informatiebeveiliging op verschillende lagen.

Toelichting:
Er zijn eisen die niet op één laag volledig zijn te realiseren. Een voorbeeld illustreert dit. Een bepaalde set gegevens dient een zeer hoge beschikbaarheid te hebben. Op de laag Inhoud worden maatregelen genomen zodat gegevens op twee, geografisch gescheiden, locaties altijd beschikbaar zijn. Alle systemen zijn dubbel uitgerust. Hieruit kan echter niet de conclusie worden getrokken dat op de transportlaag met betrekking tot Beschikbaarheid geen additionele maatregelen genomen hoeven worden. Valt de transportlaag uit, dan zijn alsnog de gegevens niet toegankelijk, ook al worden deze op twee locaties beschikbaar gesteld. In dit voorbeeld zullen op elke laag maatregelen genomen moeten worden zodat het geheel voldoet aan de beschikbaarheideisen die vanuit de gegevens worden gesteld.

Uit bovenstaand voorbeeld volgt dat er meerdere manieren zijn waarop veilige informatie-uitwisseling binnen de overheid kan plaatsvinden. Per laag zijn keuzes te maken, maar dit moet wel in samenhang gebeuren.

7.2 Wat kan de rol van Diginetwerk in relatie tot andere overheidsvoorzieningen zijn voor beveiliging van informatie-uitwisseling? Welke scenario's kunnen hierbij worden onderscheiden?

Diginetwerk voegt belangrijke waarde toe op het vlak van de beveiliging van de informatie-uitwisseling. In paragraaf 5.8 wordt specifiek aangegeven welke waarde wordt toegevoegd, onderscheiden naar de kwaliteitsaspecten B-E-I. Diginetwerk levert vooral een bijdrage aan de beschikbaarheid van informatie-uitwisseling, de bijdrage aan de exclusiviteit en integriteit is indirect: de beveiliging van Diginetwerk heeft meer effect op de beveiliging van de systemen die

zorgen voor de informatie-uitwisseling dan op de informatie-uitwisseling zelf. De Diginetwerk voorziening op zich is daarom niet toereikend om te voldoen aan de beveiligingseisen die stakeholders stellen aan veilige informatie-uitwisseling. De beveiligingsmaatregelen op de laag logistiek (bijvoorbeeld in Digikoppeling en toepassing van PKI-overheid certificaten) en op de laag Inhoud (afspraken en beveiligingsmaatregelen in applicaties en berichten) zijn onmisbaar om het gewenste beveiligingsniveau te realiseren. Diginetwerk levert weliswaar compartimentering en zonering, het beheer hiervan is verdeeld over verschillende partijen en staat niet onder directe controle van de partijen die uiteindelijk verantwoording moeten afleggen over de gegevensverwerking en beveiliging ervan. Diginetwerk levert dus wel een bijdrage aan de beveiliging, maar deze maatregelen moeten worden gezien als aanvullende maatregel.

Naast toegevoegde waarde voor de veilige informatie-uitwisseling tussen overheidspartijen levert Diginetwerk ook flexibiliteit en efficiency op door(her-)gebruik van bestaande koppelnetwerken.

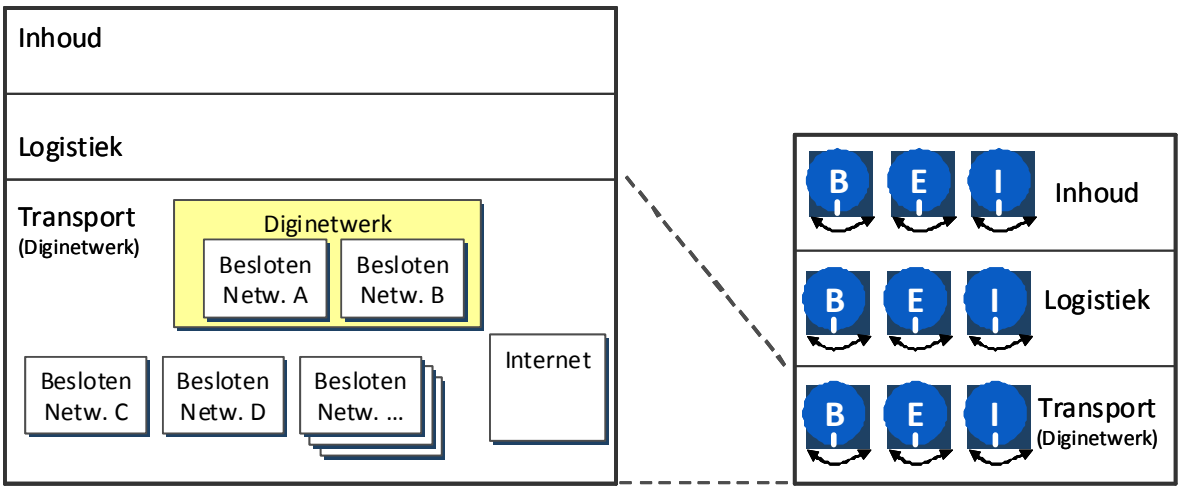
Afhankelijk van het geheel aan beveiligingsmaatregelen op de drie lagen zou Diginetwerk ook een grotere, of juist minder grote, bijdrage kunnen leveren aan de B-E-I. Om de scenario's te bepalen wordt een onderscheid gemaakt naar:

- de overwegingen met betrekking tot de invulling van B-E-I op de transportlaag.
- de IST situatie met betrekking tot de invulling van de transportlaag bij de overheid.

Bij de invulling van B-E-I op de transportlaag gelden een aantal belangrijke overwegingen:

- Generieke versus gespecialiseerde netwerken. Met “gespecialiseerd” bedoelt VKA netwerken die voor slechts één vorm van informatie-uitwisseling gebruikt worden, bijvoorbeeld mail of web services, dus gespecialiseerd op de laag Logistiek. Deze afweging betreft dus de keuze tussen een generieke netwerkvoorziening voor alle soorten toepassingen, of één of meer gespecialiseerde netwerken. De gespecialiseerde netwerken voldoen aan de specifieke eisen die aan de informatie-uitwisseling gesteld worden. Ander verkeer kan worden geblokkeerd, wat een bijdrage levert aan de beveiliging, maar niet aan de flexibiliteit en herbruikbaarheid. RINISnet is hiervan een voorbeeld. Ook Diginetwerk in de huidige opzet valt in deze categorie omdat het uitsluitend wordt gebruikt voor webservices, waarbij de koppelnetwerken beperkingen aan het verkeer opleggen. Internet daarentegen is een generieke netwerkvoorziening.
- Centrale regie versus federatief. Wordt er sterke centrale regie en toezicht uitgevoerd op de netwerkvoorziening(en), of kiest men voor een federatief model. In het laatste geval worden er wel onderling afspraken gemaakt, maar ligt de implementatie, het beheer en de controle bij meerdere partijen die elkaar daarop kunnen aanspreken. Zowel Diginetwerk als Internet hebben een federatief karakter.
- Openbaar versus besloten. Op een openbaar netwerk wordt elke partij die hieraan behoefte heeft aangesloten op het netwerk. Dit in tegenstelling tot een besloten netwerk waarbij is vastgesteld welke partijen wel, en welke niet, toegang krijgen. Diginetwerk is een besloten netwerk; Internet is openbaar.

Genoemde overwegingen hebben in het verleden geleid tot verschillende keuzes ten aanzien van de transportlaag. Binnen de overheid zijn meerdere netwerken in gebruik (IST). Zie figuur 6.



Figuur 6 Afweging van informatiebeveiliging op de transportlaag

Samengevat bestaat de transportlaag binnen de overheid uit:

- Meerdere besloten netwerken, zoals RINISnet, SUWInet, JustID, Haagsche Ring, Gemnet, etc.
- Diginetwerk, met als kenmerken logistiek specifiek, federatief en besloten.
- Internet. Ook in de huidige situatie worden er gegevens tussen overheidspartijen uitgewisseld via Internet.

Op basis van deze overwegingen en de IST situatie zijn meerdere scenario's te onderscheiden. In het kader van dit onderzoek worden drie scenario's voorgesteld. Per scenario wordt een korte beschrijving gegeven enkele in het oog springende voor- en nadelen.

Scenario	Omschrijving	Voordelen	Nadelen
1. Federatief	Dit scenario komt overeen met de huidige situatie (verschillende netwerken, waaronder Diginetwerk, met verschillende kenmerken). Beveiliging van de informatie-uitwisseling vindt op verschillende lagen plaats, afhankelijk van het toepassingsgebied.	Sneller kunnen inspelen op de individuele behoeften van organisaties. Hergebruik bestaande netwerken en bestaande (beheer-)organisaties. Handhaven van de bestaande verantwoordelijkheid-verdeling.	Naarmate het aantal partijen in de federatie groter wordt nemen de beveiligingsrisico's inherent toe. Borging van maatregelen vereist intensief overleg tussen ketenpartners. Inefficiëntie m.b.t. inzet beheerresources (meerdere beheerpartijen).

			Geen end-to-end toezicht op het naleven van beveiligingsmaatregelen. Weinig zicht op performance en beveiligingsmaatregelen bij de verschillende leveranciers.
2. Centraal	Eén netwerkvoorziening voor de overheid (met kenmerken "generiek", "centrale regie", "besloten"). Eén voorziening wil overigens niet zeggen dat dit ook (fysiek) één netwerk is. Wel is in dit scenario sprake van strakke centrale regievoering, verantwoording en toezicht. Opgemerkt wordt dat in dit scenario het Internet als optie voor de transportlaag niet verdwijnt. Ook bij één netwerkvoorziening zal de overheid gebruik maken van het Internet voor informatie-uitwisseling met partijen buiten de overheid. Door centrale regie, beheer in één hand wordt het mogelijk in dit scenario een groot aantal beveiligingsmaatregelen in de transportlaag te treffen, waardoor in minder mate gesteund hoeft te worden op maatregelen in de logistieke en de inhoud laag. Ondanks deze maatregelen zullen aangesloten partijen nog steeds maatregelen moeten nemen in hun eigen domein. Enerzijds systeembeveiliging om rekening te houden met de mogelijkheid dat systemen bij een andere overheidsinstantie zijn gehackt. Anderzijds blijven maatregelen op de lagen van logistiek en inhoud nodig om invulling te geven aan de verantwoordelijkheid die organisaties hebben t.a.v. bescherming van	Efficiënte inzet van beheerresources (één beheerorganisatie). Meerder mogelijkheden om risico's te beheersen. Eén sourcingstrategie (beter zicht op aantal en type leveranciers die diensten leveren / beheren)	Minder snel kunnen inspelen op individuele behoeften van organisaties. Meer bureaucratie. Vereist een complex organisatorisch en technisch verandertraject van alle betrokken overheden.

	persoonsgegevens.		
3. Internet	Gebruik van Internet (met kenmerken "generiek", "federatief" en "openbaar"). In dit scenario wordt veruit het grootste deel van de informatie via het Internet uitgewisseld. Alleen voor hoog risico informatie-uitwisseling (zoals bijvoorbeeld staatsgeheime informatie) wordt nog gebruik gemaakt van private verbindingen en/of besloten netwerken. Beveiliging van de informatie-uitwisseling zal in hoge mate steunen op maatregelen op de logistieke en op inhoud laag. Door de open aard van Internet is de kans dat de aangesloten systemen worden aangevallen zeer hoog. De beveiliging van alle systemen en informatiestromen moet daarom op een hoog niveau liggen.	Universeel toegang voor alle deelnemers. Veel aanbod van marktpartijen. Lage kosten van de initiële aansluiting.	Geen garanties voor beschikbaarheid en performance Risico op continuïteit (?) Elk individueel overheidsysteem / bedrijfsnetwerk moet zichzelf maximaal beschermen tegen alle mogelijke bedreigingen. Extra kosten voor treffen aanvullende beveiligingsmaatregelen op andere lagen (Geen eerste beveiligingslaag in de vorm van een besloten netwerk).

Een afweging tussen de scenario's kan uit oogpunt van informatiebeveiliging worden gemaakt door het uitvoeren van een business risicoanalyse, waarin op basis van de eisen die stakeholders stellen aan de informatiebeveiliging en in samenhang met de lagen inhoud en logistiek, de B-E-I risico's en risicobeheersmaatregelen voor de transport laag bepaald worden.

Daarbij is informatiebeveiliging niet het enige criterium. Andere criteria zijn: kosten, zorgen voor gezonde marktwerking, algemene beleiduitgangspunten zoals "gebruik generieke e-overheidsvoorzieningen" en de risico's voor het functioneren van de overheid als geheel bij uitval van de onderliggende infrastructuur.

7.3 Wat kan de positie van Diginetwerk voor informatiebeveiliging in relatie tot andere overheidsnetwerken en netwerken van private partijen, zoals Gemnet zijn?

Diginetwerk heeft een federatief karakter. De verantwoordelijkheid voor implementatie en toezicht op beveiligingsmaatregelen is verspreid over de beheerders van Diginetwerk, koppelnetwerken en van de bedrijfsnetwerken.
Er is geen overkoepelend strategisch beleids-, beveiligings- en architectuurkader voor Diginetwerk en er bestaat geen overkoepelend toezichts- en sanctiebeleid voor het naleven van de afspraken en voorwaarden.

Om de positie van Diginetwerk voor informatiebeveiliging te versterken staan twee opties open:

1. Versterken van de wederzijdse nalevings- en verantwoordingsplicht van de deelnemende partijen, met Logius als regisserende partij. Dit moet zowel gelden voor overheidspartijen als voor private partijen als Gemnet.
2. Versterken van de strategische besturing van Diginetwerk op bestuurlijk niveau, met centrale beleidskaders, toezicht, verantwoording en sancties bij niet naleving.

7.4 Wie zijn en worden de stakeholders voor aansluiting op Diginetwerk?

Stakeholders zijn organisaties binnen de overheid, de semi-overheid en particuliere organisaties met een publieke taak die op een geautomatiseerde wijze persoonsgegevens verwerken en uitwisselen en een wettelijke verplichting hebben tot het beveiligen van persoonsgegevens. Maar ook de beherende partijen van Diginetwerk en de externe leveranciers van netwerkdiensten kunnen als stakeholders beschouwd worden (zie ook paragraaf 4.1).

Indien de dienstverlening van Diginetwerk uitgebreid wordt naar bijv. het KA verkeer bij de (Rijks)overheid, of als Diginetwerk opgaat in een meer generiek overheidsnetwerk, dan kunnen ook de beleidsdepartementen stakeholder worden van dat netwerk. Hetzelfde geldt voor niet-overheidspartijen met een publieke taak.

7.5 Wat is de verwachting ten aanzien van soort en aantal aansluitingen op Diginetwerk?

Door het groeiend gebruik van e-overheidsvoorzieningen is de verwachting dat het aantal aansluitingen op Diginetwerk zal groeien. Een onzekerheid hierbij is de afweging van met name gemeentelijke organisaties om gebruik te maken van internet dienstverlening.

Voorts hangt de toekomst van het soort en aantal aansluitingen af van :

- De mate waarin huidige en toekomstige toepassingen het gebruik van Diginetwerk voorschrijven.
- De keuze om Diginetwerk open te stellen voor meerdere verkeerstypen, zoals spraak en video. Dit kan grote effecten hebben op het soort en aantal aansluiten.

Bij uitbreiding van het soort en aantal aansluitingen zal altijd de impact op de aspecten van informatiebeveiliging (B-E-I) op de transportlaag in ogenschouw genomen moeten worden. Bij een toename van het aantal organisaties dat op Diginetwerk is aangesloten neemt bijvoorbeeld de mate van "beslotenheid" van het netwerk af. Elke aangesloten partij is immers behalve potentiële uitwisselingspartner tevens potentiële bron van dreigingen tegen de B-E-I, zodat de risico's toenemen. Diginetwerk is niet gecompartimenteerd, waardoor zogenaamd "any-to-any" verkeer mogelijk is tussen de aangesloten partijen. Compartimentering door bijvoorbeeld meerdere VPN's verhoogt wel de beveiliging, maar beperkt de connectiviteit en levert een extra beheerlast op. Aan de hand van een risicoanalyse kan bij uitbreiding van het netwerk worden bepaald of de (B-E-I) risico's nog in goede verhouding staan tot het vereiste beveiligingsniveau. Daarbij geldt opnieuw de afweging tussen maatregelen per aangesloten partij en generieke maatregelen.

7.6 Welke rollen en verantwoordelijkheden (governance) zijn op strategisch-, tactisch- en operationeel niveau te onderscheiden bij de vraagsturing, de regievoering en de aanbodsturing van Diginetwerk? Wat is de rol van marktpartijen hierbij?

De rollen en verantwoordelijkheden voor de governance en het beheer van Diginetwerk zijn beschreven in paragraaf 4.4.

Voor de strategische vraagsturing door stakeholders, het strategisch beheer door het ministerie van BZK en de strategische aanbodsturing door de belangrijkste leveranciers zijn geen rollen en verantwoordelijkheden gedefinieerd en ingevuld. Dit houdt ook in dat de IT-governance van Diginetwerk, zoals omschreven door de Algemene Rekenkamer, niet is ingevuld. Er vindt geen bestuurlijke afstemming plaats over het strategisch beleid. Er is geen sourcingstrategie ontwikkeld voor marktpartijen als Gemnet. Er is geen bestuurlijk beveiligingsbeleid geformuleerd en er vindt geen bestuurlijk toezicht en verantwoording plaats op de naleving van beleids- en beveiligingsregels.
Bij de aanbodsturing van Diginetwerk door marktpartijen speelt KPN als netwerkdienstverlener een dominante rol als marktpartij. Binnen OT2006data is naast KPN ook BT een netwerkdienstverlener.
De marktpartij Gemnet, een volle dochter van KPN, vervult de rol van koppelnetbeheerder en volgt de aansluitvoorwaarden van Diginetwerk. Gemnet voert daarbij een eigen commerciële koers en kent daarbij weinig concurrentie.

Op tactisch niveau heeft Logius het initiatief genomen tot het organiseren van de tactische vraagsturing door de stakeholders (de z.g. 'kleine governance') en draagt zorg voor het tactisch beheer. Dit houdt in dat Logius veranderbehoeften bij stakeholders analyseert, de (technische) architectuur van Diginetwerk beheert en onderhoudt, zorg draagt voor het tactische beveiligingsplan en zorg draagt voor aansluitvoorwaarden en dienstverleningsafspraken met ketenpartijen als BKWI, Gemnet. Daarnaast voeren de ketenpartners BKWI en Gemnet zelfstandig tactisch beheer over hun de koppelnetwerken.
Zoals eerder in dit rapport uiteengezet ligt ook een belangrijke verantwoordelijkheid voor de beveiliging van Diginetwerk bij de organisaties die via een koppelnetwerk op Diginetwerk zijn aangesloten (zoals uitvoeringsorganisaties en gemeenten). Het zijn de bedrijfsnetwerken van deze organisaties die op het koppelnetwerk / Diginetwerk worden aangesloten. Het beheer over deze bedrijfsnetwerken is in de praktijk vaak uitbesteed. Deze beheerpartijen (marktpartijen) spelen hierdoor, gelet op het belang van een goede beveiliging van de bedrijfsnetwerken voor Diginetwerk, een rol in het totale beheer van Diginetwerk. Logius heeft geen toezichthoudende rol op deze beheerders.

Op operationeel niveau draagt BKWI zorg voor het beheer van het Basiskoppelnetwerk (BKN). Logius en BKWI hebben hierover een samenwerkingsovereenkomst gesloten. Dit houdt in het technisch ondersteunen van afnemers, het monitoren van de performance en de beveiliging van het netwerk, het afhandelen van incidenten en het doorvoeren van wijzigingen in de netwerk infrastructuur. BKWI maakt voor het operationele beheer gebruik van een onderaannemer.

De koppelnetwerk beheerders voeren verder zelfstandig het operationele beheer over hun eigen netwerken.

7.7 Wat is de rol van Diginetwerk in relatie tot de visie vorming in kavel 7 (Basisinfrastructuur)?

Diginetwerk past goed binnen het concept van een generieke dienst 'Basisinfrastructuur' en connectiviteit van netwerken.
De visie op de connectiviteit voor het Rijk gaat uit van een netwerk van netwerken, dat op basis van overeengekomen (rijks-)standaarden (op gebied van connectiviteit en veiligheid) gekoppeld zijn. De visie heeft daarmee elementen van de in dit rapport genoemde scenario's federatief en centraal. De visie onderkent enerzijds de inherente diversiteit binnen de overheid, waardoor meerdere netwerken naast elkaar bestaan en geeft ook het belang aan van meer strategische en tactische regievoering op gemeenschappelijke vraagbundeling, kaderstelling en sturing, ondermeer door generieke, rijksbrede (technische) kaders voor een generieke ICT-voorziening voor de rijksoverheid.
De visie is primair geschreven vanuit de rijkstaken, met de mogelijkheid om, waar mogelijk, samenhang te realiseren met de basisinfrastructuur van de gehele overheid. Dit draagt ook bij aan hergebruikt van overheidsvoorzieningen.
Diginetwerk is enerzijds breder, omdat de dienstverlening zich richt is op de gehele overheid. Diginetwerk is echter ook smaller in die zin dat het zich alleen richt op dataverkeer tussen organisaties, terwijl het netwerk voor de rijksoverheid bedoeld is voor data, spraak en video. Een basisinfrastructuur die aan zowel aan de behoeften van de Rijksoverheid als aan de behoeften van de Diginetwerk stakeholders kan voldoen moet daarom intern open en transparant zijn en voldoende bandbreedte bieden om de prestatie-eisen van verschillende verkeersstromen te faciliteren.
De visie onderkent het vraagstuk van de huidige geringe marktwerking bij Diginetwerk en streeft een verkaveling na die bijdraagt aan een meer evenwichtige mededinging.
Diginetwerk kan vanuit haar ervaring met de implementatie en het beheer van een (virtueel) overheidsnetwerk een richtinggevende rol spelen bij de visievorming.

7.8 Hoe kan het TopLevelDomein (TLD) .overheidnl hierbij benut worden?

De meeste respondenten zagen in een overheids-TLD niet direct een middel om de beveiliging te verbeteren. Indien de beveiliging van de name-server die dit domein gaat servicen, minder strikt is dan de beveiliging van de als zeer veilig aangeschreven servers van SIDN (van het .nl domein) zou het effect zelfs negatief kunnen zijn. Ook als DNSSEC wordt toegepast, is het noodzakelijk dat het beheer en de beveiliging van DNS servers op hoog niveau zijn ingericht, omdat ze een gewild doel van aanvallen zijn.

De visie van VKA op dit punt is als volgt.
Doordat de overheid zelf het volledige beheer krijgt over alle gebruikte name-servers, tot en met TLD, kan de beveiliging van informatie-uitwisseling tussen overheidsorganisaties die momenteel verschillende domeinen onder .NL gebruiken, in lichte mate versterkt worden. Voorwaarde daarbij

is dat het beheer van .overheidnl TLD op minimaal hetzelfde kwaliteitsniveau ligt als van het huidige .NL. Ook zou eigen beheer mogelijk een voordeel kunnen zijn in een situatie waarin de nationale veiligheid in het geding is. Het is echter ook denkbaar dat de overheid voor die situaties het gezag over .NL borgt. Voor gebruikers binnen de overheid zou .overheidnl dus een klein voordeel kunnen bieden ten opzichte van .overheid.NL. Gebruikers afkomstig uit een domein buiten de overheid zullen nog altijd door een name-server buiten de Nederlandse overheid verwezen worden. Waar een gebruiker binnen .NL door de name-servers van SIDN naar overheid.NL wordt verwezen, zal dit bij een TLD .overheidnl gebeuren door de 10 internationale root name-servers, die niet door Nederlandse partijen beheerd worden. Voor de burger en het Nederlandse bedrijfsleven zou het effect dus zelfs negatief kunnen zijn. De verschillen in betrouwbaarheid bij toepassing van een .overheidnl TLD zijn dus subtiel en op basis van de huidige inzichten is er geen duidelijk positief of negatief effect te onderscheiden.

Enkele respondenten achten het mogelijk dat een eigen overheids-TLD een onderdeel kan zijn binnen een architectuur voor de overheidsinformatievoorziening, die als geheel een sterkere mate van beheersing over alle aspecten van informatiebeveiliging biedt. Op dit moment ligt er echter niet een dergelijk architectuurontwerp klaar. Dit zou mogelijk een nuttig onderwerp van studie zijn..

7.9 Welke overwegingen en randvoorwaarden voor de inrichting van de besturing, beheer en de financiering van de exploitatie van Diginetwerk gelden er bij de verschillende scenario's voor de beveiliging van informatie-uitwisseling binnen de overheid?

De verschillende scenario's voor de vormgeving van de transportlaag leiden tot ander accenten in de besturing, het beheer de financiering. In onderstaand schema worden een aantal overwegingen en randvoorwaarden per scenario uitgewerkt.

Scenario	Besturing	Beheer en beveiliging	Financiering
1. Federatief	Versterken van de ketenafspraken tussen de deelnemers van Diginetwerk.	Uitwerken van de wederzijds afspraken over rechten, plichten en naleving , gebaseerd op BIR of ISO 27002.	Gedeeltelijk centraal. Gedeeltelijk bijdragen door afnemers.
2. Centraal	Diginetwerk verplicht stellen voor alle informatie-uitwisseling. Een wettelijke grondslag overwegen. Versterken en bewaken van de marktwerking.	Bepalen van centrale beleidskaders, bijvoorbeeld toezicht op naleving en verantwoording, gebaseerd op BIR of ISO 27002, Onderscheid tussen strategisch, tactisch en operationeel beheer.	Centrale financiering van de generieke infrastructuur. Eventueel aangevuld met bijdragen voor gebruik door afnemers.
3.	Mantel contracten met	Afspraken met marktpartijen	Door afnemers,

Internet	marktpartijen.	over beheer- en beveiligingsmaatregelen en het toezicht en de naleving daarvan. Eisen stellen aan beheer en beveiliging op de lagen inhoud en logistiek.	afhankelijk van gebruik.

A Begeleidingscommissie

Organisatie	Naam
Ministerie van BZK DG BK Directie Burgerschap & Informatiebeleid	Michiel Schoo (voorzitter) Arnold Reinders
Ministerie van BZK DGOBR Directie Informatiseringsbeleid Rijksdienst	Leon-Paul de Rouw
Ministerie van BZK DG BK Bureau Verkenningen & Onderzoek	Marjolijn Blom
Logius	Alexander Hielkema

B Geraadpleegde documentatie

- Diginetwerk Architectuur, Logius, versie 0.99, 15 november 2010
- Aansluitvoorwaarden Diginetwerk, Logius, versie 1.71, 16 december 2010
- Netwerktekening,Logius, "Diginetwerk totaal", versie 0.1f, 10-08-2011
- Dienstbeschrijving Diginetwerk, Logius, versie 1.2, 4 oktober 2010
- Dossier Afspraken en Procedures Diginetwerk, Logius, versie 1.0, 28 juni 2012
- Presentatie Aansluiting op Diginetwerk 2011, Gemnet
- Een toekomstvast Rijksnetwerk, BZK, concept, 10 okt 2012 ICCIO
- Marktspiegel ON 2013, BZK, versie 2.0, 14 augustus 2012
- Baseline Informatiebeveiliging Rijksdienst TNK, BZK, versie 0.99ka, 9 aug 2012
- IB Patronen, PvIB, 1.0, 11 juni 2012
- Normenkader IB Rijksweb, BZK, versie 13.3, 5 april 2006
- SLA BKWI Basiskoppelnet, BKWI, versie 1.1, 18 augustus 2010
- Samenwerkingsovereenkomst BKWI-Logius basiskoppelnetwerk Diginetwerk, versie 1.0, 10 september 2010
- Referentiekader informatiebeveiliging aansluitvoorwaarden Haagse Ring, Logius, versie 1.1, 11 oktober 2006
- NORA, versie 2.0, 25 april 2007
- NORA, versie 3.0, 29 september 2010
- NORA Dossier Informatiebeveiliging, versie 1.3, 1 september 2010
- Vraag inzake gebruik stelselvoorzieningen en –standaarden, BZK, januari 2012
- Memo Samenhang aansluitvoorzieningen basisregistraties, Logius, 7 september 2011
- Impactanalyse Digikoppeling, KING, versie 1.0, 27 juni 2012
- Achtergrondstudies en verkenningen 23, Registratiekamer, april 2001
- Grip op informatievoorziening IT Governance ministeries, ARK, Tweede Kamer, vergaderjaar 2005–2006, 30 505, nrs. 1–2
- Besturingsmodel regie en Sourcing voor de generieke ICT van de Rijksdienst (TBGI), ICCIO/Subcommissie Regie en sourcing, versie concept, 2 september 2010

Naast deze documenten zijn op internet nog diverse factsheets over de netwerkdienstverlening van de verschillende betrokken partijen bestudeerd.

C Lijst van gesprekspartners

Organisatie	Gesprekspartner(s)
Logius	Alexander Hielkema Cees van der Poel
BKWI	Evert Jan Rietbergen
RINIS	Rob Verweij Hans Sinnige
Gemnet	Paul Bloemers Bertrand van Deutecom
BPR	Peter Provily Hans van Laar Peter van Damsteeg
Belastingdienst	Chris van der Raadt Ger van Berlo Saco Bekius
DUO	Kor Brandts
BZK Stelsel van basisregistraties	Anton van Weel
BZK DGOBR/DIR	Roel van Beelen Carl Adamse
KING	Ton van Laarhoven
VNG	Kees Duijvelaar
NCSC	Rene Visser Edwin Tump Ton Slewe
NORA	Jaap van der Veen

D NORA Normen IB (uit Diginetwerk Architectuur)

Principe
ICT-voorzieningen zijn in zones ingedeeld.
Definitie
Een zone is een afgebakend netwerk van ICT-voorzieningen, waarbinnen gegevens vrijelijk kunnen worden uitgewissseld. Informatie-uitwisseling met andere zones verloopt via koppelvlakken.
Toelichting
Het primaire doel van zonering is isolatie van risico's, waardoor bedreigingen en incidenten in de ene zone niet doorwerken in een andere. Hierbij gaat het er niet alleen om de interne tegen de externe, onvertrouwde zone te beschermen, maar ook om interne zones, zoals bijvoorbeeld ontwikkeling, test, acceptatie en productieomgevingen, van elkaar te scheiden.
Zonering maakt het voorts mogelijk om met verschillende beveiligingsniveau's binnen een infrastructuur te werken en informatiestromen en risicovolle beheercommando's te reguleren. Deze toegangbeperking is soms krachtiger dan toegangsbeveiliging via aanlogprocedures bij servers. Zonering maakt het netwerk overzichtelijker voor beheer en dat is tevens van belang voorbeveiliging.
Elke zone kent dus andere risico's samenhangend met de diensten of ICT-voorzieningen die erin opgenomen zijn. Binnen zones kunnen met standaard maatregelen sub-zones worden ingericht als het risicoprofiel dat vereist, bijvoorbeeld om verschillende productieomgevingen uit elkaar te houden, die niet het zelfde beveiligingsniveau hebben. Externe netwerken worden in dit zoneringsconcept ook als aparte zone gezien.
De controle op informatiestromen tussen zones wordt verzorgd door zogenaamde filterfuncties, die als aparte IB-functie worden gezien.
Bij end-to-end beveiliging waarbij de berichten of documenten zelf beveiligd zijn, zal minder filtering noodzakelijk zijn, maar dat doet vooralsnog niets af aan het zoneringsconcept.
Zonering heeft betrekking op het geheel van de ICT-voorzieningen
Motivering
Door zonering kunnen risico's worden geïsoleerd, waardoor bedreigingen en incidenten die optreden in de ene zone niet doorwerken in een andere zone.

Eisen te stellen aan zones

Doelstelling van de maatregel
Zones zijn als eenheid van beveiliging en beheer gedefinieerd.
Implementatierichtlijnen
1. Elke zone heeft een vastgesteld beveiligingsdoel.
2. Elke zone wordt slechts beheerd onder verantwoordelijkheid van een beheerinstantie (m.u.v. onvertrouwde derden).
3. Een zone heeft een gedefinieerd beveiligingsniveau, d.w.z. kent een gedefinieerd stelsel van samenhangende beveiligingmaatregelen.
4. De maatregelen van logische toegangsbeperking zijn van toepassing op alle ICT-voorzieningen in een zone.
5. Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.
6. Zones kunnen worden onderscheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen (Code 11.4.7), door toepassing van verschillende protocollen, encryptietechnologie, partitionering van servers, maar ook door fysieke scheiding
7. Zonering wordt ingericht met voorzieningen, waarvan de functionaliteit is beperkt tot de strikt noodzakelijke (hardening van voorzieningen).
8. Bij elkaar behorende serverfuncties bevinden zich slechts in één zone.

Filtering

Principe
Op het koppelvlak tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens.
Definitie
Het doel van filtering is bescherming van zones tegen het doorlaten van Denial of Service attacks, indringers, ongewenste inhoud, virussen en informatie lekkage.
Toelichting
Filtering controleert in- en uitgaande gegevensstromen op locatie, vorm (protocol) of inhoud van gegevensstromen, afhankelijk van de aard van de stromen en zones. Filtering controleert geen identiteiten van individuele gebruikers. De communicatie tussen twee zones wordt getoetst op ongewenst gedrag. Daarvoor wordt een elektronisch profiel vastgelegd van de zenders in de betrokken zones. Van het communicatiegedrag wordt elektronisch een 'reputatie score' vastgelegd, dat enerzijds wordt vergeleken met het beleidsregels voor doorlaten van communicatie en anderzijds met bekende patronen van ongewenste communicatie.
Motivering
Filterfuncties zijn onlosmakelijk verbonden aan het principe van zonering en ontlenen daaraan ook hun motivatie.