Onderzoek veiligheid diensten in de Digitale Agenda.nl

Eindrapport

Auteur	Team Collis/HEC
Versie	1.0
Datum	8-03-2012
Status	Definitief

Documentgegevens

Opdrachtgever	Ministerie van EL&I, mevr. dr. L.M.N. Kroon, directeur regeldruk en ICT beleid
Projectmanager	Henk van Dam, Collis
Projectcode	Collis_2011_832
Document titel	Onderzoek veiligheid diensten in de Digitale Agenda.nl Eindrapport
Bestandsnaam	Eindrapportage_Onderzoek_diensten_MinELI_versie_1_0.docx
Archief naam	
Trefwoorden	ICT, veiligheid, Ministerie van EL&I, onderzoek, Regelhulp, OndernemingsDossier, SBR, eFactureren, eHerkenning, OndernemersPlatform, Dienstenloket / Antwoordvoorbedrijven, Berichtenbox, Open Data, Digipoort
Status	Definitief
Verspreiding	Ministerie van EL&I

Onderzoekers	ir. P.J.M. Hin, CISA dr. J.M.E. Geers dr. P. Nijsse drs. M. Radema dr. M. Spruit

Collis BV
De Heyderweg 1
2314 XZ LEIDEN
The Netherlands
Tel. +31 71 581 36 36
Fax +31 71 581 36 30
E-mail info@collis.nl
Website www.collis.nl

Versieoverzicht

Versie	Datum	Status	Auteur
1.0	8-03-2012	Definitief	Collis HEC team

Wijzigingshistorie

Versie	Datum	Reden wijziging
1.0	8-03-2012	Eindconcept geakkordeerd door opdrachtgever

INHOUDSOPGAVE

MANAGEMENTSAMENVATTING 6

A. SAMENVATTING ONDERNEMINGSDOSSIER 10
B. SAMENVATTING SBR EN EFACTUREREN (INCLUSIEF DIGIPOORT-PI) 12
C. SAMENVATTING EHERKENNING 15
D. SAMENVATTING ANTWOORDVOORBEDRIJVEN INCLUSIEF ONDERNEMERSPLATFORM EN OPEN DATA 18

1 INLEIDING 21

1.1 DOELGROEP 21
1.2 LEESWIJZER BIJ DIT DOCUMENT 21

2 OPDRACHT 22

2.1 KADER VAN DE OPDRACHT 22
2.2 OPDRACHT EN WERKWIJZE 23
2.2.1 Opdracht 23
2.2.2 Werkwijze 24

3 RISICO- EN BEOORDELINGSKADER 25

4 BEOORDELING PER DIENST 27

4.1 ENKELE WAARNEMINGEN VOORAF 27
4.2 REGELHULP 28
4.2.1 Korte beschrijving 28
4.2.2 Conclusie / aanbevelingen 28
4.2.3 Samenvatting 28
4.3 ONDERNEMINGSDOSSIER 29
4.3.1 Korte beschrijving 29
4.3.2 Risicoprofiel 30
4.3.3 Bevindingen 30
4.3.4 Oordeel 33
4.3.5 Aanbevelingen 33
4.3.6 Samenvatting 34
4.4 STANDAARD BEDRIJFSRAPPORTAGE (SBR) EN EFACTUREREN 36
4.4.1 Korte beschrijving 36
4.4.2 Risicoprofiel 39
4.4.3 Bevindingen 40
4.4.4 Oordeel 43
4.4.5 Aanbevelingen 45
4.4.6 Samenvatting 46
4.5 EHERKENNING 49
4.5.1 Korte beschrijving 49
4.5.2 Risicoprofiel 51

4.5.3 Bevindingen 51
4.5.4 Oordeel 53
4.5.5 Aanbevelingen 54
4.5.6 Samenvatting 55
4.6 **ANTWOORDVOORBEDRIJVEN (INCL ONDERNEMERSPLATFORM EN OPEN DATA) 59**
4.6.1 Korte beschrijving 59
4.6.2 Risicoprofiel 60
4.6.3 Bevindingen 61
4.6.4 Oordeel 63
4.6.5 Aanbevelingen 63
4.6.6 Samenvatting 63
4.7 **BERICHTENBOX 65**
4.7.1 Korte beschrijving 65
4.7.2 Risicoprofiel 67
4.7.3 Bevindingen 67
4.7.4 Oordeel 69
4.7.5 Aanbevelingen 70
4.7.6 Samenvatting 70

5 CONCLUSIE 73

6 REFERENTIES 76

APP 1 INITIEEL OPGEVRAAGDE DOCUMENTATIE 78

APP 2 SELECTIE VAN STANDAARDEN OP GEBIED VAN INFORMATIEVOORZIENING 80

APP 2.1 ARCHITECTUURSTANDAARDEN 80
APP 2.2 INFORMATIE-ARCHITECTUUR STANDAARDEN 80
APP 2.3 BEDRIJFSARCHITECTUUR STANDAARDEN 81
APP 2.4 STANDAARD OP HET GEBIED VAN BEHEER 81
APP 2.5 INFORMATIEBEVEILIGING STANDAARDEN 81

APP 3 CONTACTMOMENTEN EN GERAADPLEEGDE DOCUMENTATIE 83

APP 3.1 REGELHULP 83
APP 3.2 ONDERNEMINGSDOSSIER 83
APP 3.3 STANDAARD BEDRIJFSRAPPORTAGE (SBR) EN EFACTUREREN 84
APP 3.4 EHERKENNING 85
APP 3.5 ANTWOORDVOORBEDRIJVEN INCLUSIEF ONDERNEMERSPLATFORM EN OPEN DATA 86
APP 3.6 BERICHTENBOX 86

APP 4 VRAGENLIJST 88

APP 4.1 INLEIDENDE ALGEMENE VRAGEN 88
APP 4.2 VEILIGHEIDSVRAGEN 88

MANAGEMENTSAMENVATTING

Opdracht
Dit document beschrijft de uitkomst van een onderzoek dat in opdracht van het Ministerie van Economische Zaken, Landbouw en Innovatie (in het vervolg afgekort tot Ministerie van EL&I) is gedaan door Collis en HEC ten aanzien van de veiligheid van de diensten uit de Digitale Agenda.nl. Dit onderzoek heeft plaatsgevonden in november 2011.

De negen diensten zijn: Regelhulp, OndernemingsDossier, Standaard Bedrijfsrapportage (SBR), eFactureren, eHerkenning, Antwoordvoorbedrijven, Ondernemersplatform, Open Data en Berichtenbox. Regelhulp is in overleg met de opdrachtgever buiten scope geplaatst, omdat er nog geen ontwerp of werkend systeem . De voor SBR en eFactureren noodzakelijke dienst Digipoort-PI is in het onderzoek meegenomen.

De vragen, die het Ministerie van EL&I beantwoord wilde zien door middel van het onderzoek, zijn:

A. Is het ontwerp (inrichting, proces en beheer) van de elektronische overheidsdiensten die beschreven zijn in de Digitale Agenda.nl veilig?
    1. Is er een risicoanalyse gemaakt?
    2. Welke maatregelen zijn er in het ontwerp van de diensten genomen om veiligheid te borgen?
    3. Welke maatregelen zijn of worden in de beheerfase van de diensten genomen om de veiligheid te borgen?
    4. Dekken de maatregelen de risico's voldoende af, c.q. is de risicoanalyse betrouwbaar?
B. Is de feitelijke werking van de diensten veilig?
    1. Worden de maatregelen in het ontwerp en de beheerfase van de diensten in de praktijk uitgevoerd door betrokken stakeholders en zowel in de front- als de backoffice (voor zover de dienst reeds operationeel is) en wie controleert dit?
    2. Dekken de maatregelen de risico's voldoende af, c.q. is de risicoanalyse betrouwbaar, c.q. vragen operationele tekortkomingen om aanvullende maatregelen?

Enkele waarnemingen vooraf
Door de geïnterviewden is kwalitatief goede input gegeven; men is bovendien sterk betrokken bij het onderwerp. De voor het onderzoek benodigde documentatie had wat eerder kunnen worden verstrekt. Bij het verstrekken van de informatie aan de onderzoekers blijkt dat in enkele gevallen gebruik is gemaakt van faciliteiten van private (gratis) aanbieders voor het versturen van overheidsinformatie. De onderzoekers raden het gebruik van dergelijke faciliteiten af.

Risicoprofielen van de te onderzoeken diensten
De veiligheid van een dienst wordt bepaald door de beschikbaarheid ervan, door de (data)integriteit en de vertrouwelijkheid. In het onderzoek hebben de onderzoekers voor iedere dienst een risicoprofiel geformuleerd en afgestemd met de geïnterviewden van de betreffende dienst. Uit het risicoprofiel blijkt welke eisen de dienst stelt op het gebied van beschikbaarheid, (data)integriteit en vertrouwelijkheid. De verschillende diensten hebben verschillende risicoprofielen. Een deel van de diensten stelt lage tot middelmatige eisen aan de beschikbaarheid, (data)integriteit en vertrouwelijkheid. Dit zijn OndernemingsDossier, SBR, eFactureren, Ondernemersplatform, AntwoordvoorBedrijven en Open Data.

Een ander deel van de diensten stelt hoge eisen aan de beschikbaarheid, (data)integriteit en vertrouwelijkheid. Dit zijn eHerkenning, Berichtenbox en Digipoort-PI (als onderdeel van SBR en eFactureren). eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij (overheids)dienstverleners en Berichtenbox en Digipoort-PI zijn informatieuitwisselings-diensten tussen burgers, bedrijven en overheidsdienstverleners. Vanwege het hiervoor noodzakelijke vertrouwen bij de gebruikers, moet de veiligheid van deze diensten zeer goed op orde zijn.

Clustering
In het onderzoek zijn enkele diensten geclusterd of apart benoemd. Antwoordvoorbedrijven is in het onderzoek geclusterd met Ondernemersplatform en Open Data vanuit het oogpunt van verwantschap. SBR en eFactureren maken samen gebruik van een voor de dienst essentiële infrastructuur Digipoort-PI en zijn tevens geclusterd. Berichtenbox is organisatorisch ondergebracht bij Antwoordvoorbedrijven, maar wordt in dit onderzoek apart behandeld onder Berichtenbox.

Beoordeling per dienst / cluster diensten in het kort
De kort samengevatte beoordeling per dienst, of cluster van diensten, is als volgt:

- **OndernemingsDossier:** In het huidige beginstadium lijkt het OndernemingsDossier veilig, zoals uitgevoerd onder de verantwoordelijkheid van de initiatiefnemende branches. Een integrale governance met duidelijke veiligheidsparagraaf voor de samenwerking tussen overheid en het bedrijfsleven is noodzakelijk voor verder groei van het ondernemingsdossier. Hierin moet bijvoorbeeld de vraag worden beantwoord wie onderzoek gaat uitvoeren naar en eisen moet stellen aan de veiligheid van een ondernemingsdossier. De verantwoordelijkheden van EL&I en private marktpartijen dienen expliciet te worden gemaakt.
- **Cluster Standaard Bedrijfsrapportage (SBR) en eFactureren, inclusief Digipoort-PI:** Voor Digipoort-PI zijn veiligheid en beheer goed geregeld. SBR en eFactureren zijn afsprakenstelsels. Voor SBR en eFactureren is het eigenaarschap niet goed uitgekristalliseerd, maar de veiligheid is niet direct in het geding. De risico's voor SBR en eFactureren, voor zover deze betrekking hebben veiligheid, vallen binnen Digipoort-PI.
- **eHerkenning**: Het ontwerp van de besturing-, beheer- en beveiligingsprocessen op stelselniveau is voor de transitiefase voldoende veilig, zij het niet overtuigend. Aanvullende zekerstelling is gewenst, met name door onafhankelijke review van de risicoanalyses en het bepalen of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn. Daarnaast zou er vaart gemaakt moeten worden met de transitie naar de definitieve beheerfase bij Logius. De ontworpen (deels tijdelijke) processen en de maatregelen uit het normenkader lijken op deelnemer- en stelselniveau goed geïmplementeerd te zijn, maar er vindt onvoldoende monitoring plaats op het implementeren van wijzigingen en nieuwe maatregelen. Dit kan leiden tot incidenten op het gebied van veiligheid. Voor de borging van de veiligheid op termijn is het nodig om het ontwerp van de processen op stelselniveau te verbeteren, het implementeren van wijzigingen en nieuwe maatregelen effectief te monitoren en regelmatig een uitgebreide stelselaudit uit te voeren in opdracht van de beleidsopdrachtgever van eHerkenning.
- **Cluster Antwoordvoorbedrijven (inclusief Ondernemersplatform en Open Data)**: Cluster Antwoordvoorbedrijven heeft voldoende aandacht voor veiligheid in de vorm van testen, ontwerpen en Threat and Vulnerability Analysis (TVA's).
- **Berichtenbox (BBvB)**: Voor nu is de berichtenbox technisch veilig. Op uitvoeringsniveau zijn acties (*code reviews*[1] en penetratietesten) uitgevoerd en opgevolgd om de veiligheid te bevorderen.

[1] Code reviews: systematisch onderzoek naar broncode van software programma's

Echter het ontwerp van de de besturing-, beheer en beveiligingsprocessen is niet voldoende uitgewerkt waardoor de veiligheid niet structureel is geborgd. Structurele aandacht voor de veiligheid dient te worden geborgd nu duidelijk is dat de Berichtenbox in elk geval in 2012 operationeel blijft. Doordat het ontwerp van de besturing-, beheer en beveiligingsprocessen niet voldoende is uitgewerkt zijn mogelijk noodzakelijke beveiligingsmaatregelen over het hoofd gezien. De implementatie van de processen en maatregelen uit het ontwerp is nog niet getoetst door middel van een audit. Daardoor is het onduidelijk in hoeverre de implementatie is afgerond. De mogelijke tekortkomingen in het ontwerp van de besturing-, beheer- en beveiligingsprocessen en het ontbreken van regelmatige audits in opdracht van de eigenaar van de dienst dienen met spoed te worden opgepakt om de veiligheid van deze dienst op korte termijn al sterk te verbeteren en te borgen.

Is het ontwerp van de diensten veilig?
Bij de drie diensten die hoge eisen stellen op het gebied van veiligheid, is het aspect veiligheid (eHerkenning, Berichtenbox en Digipoort-PI) een belangrijk criterium geweest in het o*ntwerp van d*e dienst en het beheer ervan. Bij Digipoort-PI heeft dit geleid tot een veilige dienst. Bij eHerkenning en Berichtenbox zijn er onvolkomenheden op het gebied van governance en continuïteit van de beheerorganisatie. Daarnaast ontbreken in het ontwerp van deze twee diensten een aantal beveiligingsmaatregelen dat de veiligheid van deze diensten op termijn verbetert. Ten tijde van het onderzoek was eHerkenning voldoende veilig, maar niet overtuigend. Door de genoemde onvolkomenheden kan voor de langere termijn geen veilige werking gegarandeerd worden. Voor Berichtenbox is het van belang op korte termijn vast te stellen of dit het geval is door het uitvoeren van een gap analyse en controle bij de uitvoerende partijen.

Bij de diensten die lage tot middelmatige eisen stellen, krijgt beveiliging in het ontwerp van de dienst en het beheer ervan minder aandacht, maar dat is ook reëel en het beoogde beveiligingsniveau is voor deze diensten voldoende.

Bij iedere dienst is een restrisico aanwezig. Het is namelijk niet haalbaar en niet betaalbaar om de risico's voor de dienst tot nul te reduceren. De eigenaar van de dienst bepaalt welke kosten voor het beveiligen van de dienst nog redelijk zijn, en daarmee welk restrisico acceptabel is. Dit betekent echter dat bij het volledig en correct implementeren en uitvoeren van alle beoogde beveiligingsmaatregelen, toch een beveiligingsincident op kan treden. Het restrisico voor de dienst moet bewust geaccepteerd en vastgelegd worden door de eigenaar van de dienst. Voor geen van de onderzochte diensten, behalve Digipoort-PI, is echter het restrisico bepaald, geaccepteerd en vastgelegd door de eigenaar ervan.

Is de feitelijke werking veilig?
Bij alle operationele diensten zijn de beoogde beveiligingsmaatregelen getroffen, maar niet voor alle diensten wordt dit goed gemonitoord. Alleen voor Digipoort-PI is er afdoende monitoring op het implementeren van beveiligingsmaatregelen. Onzorgvuldigheid bij de naleving van beveiligingsmaatregelen kan al op korte termijn tot incidenten leiden. De aanbeveling is om op korte termijn te investeren in het beter monitoren van het implementeren van beveiligingsmaatregelen. Daarnaast is voor Berichtenbox op korte termijn een audit op de kwaliteit en het naleven van de procedures en beveiligingsmaatregelen noodzakelijk.

Om de veiligheid van de diensten op termijn zeker te kunnen blijven stellen, zijn verbeteringen en uniformering in auditing en aanvullende technische maatregelen nodig. Voor wat betreft de veiligheid

van de diensten is er geen overheidstoezicht vanwege het ontbreken van een wettelijk kader hiervoor. De beleidsverantwoordelijken hebben gekozen voor controle via auditing. Voor alle operationele diensten wordt gebruik gemaakt van auditing (behalve bij Berichtenbox) en penetratietesten. Bij auditing wordt echter te veel vertrouwd op audits waarvan de onderzoekers vinden dat de uitvoerders van de diensten de scope en diepgang van de audits te veel zelf kunnen beïnvloeden. Dit is vooral een aandachtspunt voor de diensten die hoge eisen stellen op het gebied van veiligheid (eHerkenning, Berichtenbox en Digipoort-PI). Het uitgangspunt zou dan ook moeten zijn dat voor deze diensten de opdrachtgever van de dienst, de scope en diepte voor de audits bepaalt.

Bij penetratietesten wordt te veel vertrouwd op de volledigheid van deze testen. Penetratietesten geven echter een beperkte toetsing op het gebied van veiligheid. Penetratietesten zijn bedoeld als aanvulling op andere beveiliging- en toetsingsmaatregelen. De beheerders van diensten die hoge eisen stellen op het gebied van veiligheid (eHerkenning, Berichtenbox en Digipoort-PI) zouden moeten overwegen om meer gebruik te maken van systemen die hackers kunnen detecteren en andere proactieve technische maatregelen om operationele risico's te verkleinen.

Verantwoording onderzoek

De onderzoekers hebben in hun onderzoek naar het ontwerp en de feitelijke werking van de veiligheid van de diensten in de Digitale Agenda.nl de risicoprofielen meegewogen in de diepte van het onderzoek. Daar waar de onderzoekers het noodzakelijk vonden is aanvullende documentatie op locatie ingezien en zijn bijvoorbeeld certificaten gecontroleerd. Daarnaast bleek tijdens het onderzoek dat bij de meeste diensten recent audits en penetratietesten waren uitgevoerd. Er is voor gekozen deze niet opnieuw uit te voeren. Bij private partijen zijn geen controles gedaan.

Samenvattingen betreffende de onderzochte diensten

Per dienst of cluster van diensten is op de volgende bladzijden een samenvatting gegeven van het risicoprofiel, de beantwoording van de onderzoeksvragen, de conclusie en aanbevelingen.

A. Samenvatting OndernemingsDossier

Inleiding:
Het Ministerie van EL&I faciliteert de totstandkoming van het OndernemingsDossier en stelt door middel van algemene referentiearchitectuur standaarden voor. Het OndernemingsDossier is een initiatief en de verantwoordelijkheid van de deelnemende branches. Er zijn door de onderzoekers gesprekken gevoerd om een beeld van de veiligheid op te bouwen.
Het OndernemingsDossier is in het beginstadium. Eind 2012 worden 5000 aangesloten ondernemers verwacht. Het OndernemingsDossier wordt om te beginnen ingevoerd bij drie koploperbranches, (horeca, recreatie en rubber- en kunststofindustrie). Gestart wordt met 46 bedrijven, 11 gemeenten, 2 provincies en 2 rijksinspecties (eind 2011). Overheden hebben(op basis van autorisatie en toestemming van de ondernemer) inzage in de kwalitatieve gegevens.

Risicoprofiel van de dienst:
De veiligheidsaspecten van het OndernemingsDossier hebben voornamelijk te maken met de classificatie van de opgeslagen gegevens, het beschermen ervan en het organiseren van de toegang voor ondernemers en overheidsorganisaties. Daartoe maakt het OndernemingsDossier voor identificatie en authenticatie van alle gebruikers nu gebruik van eHerkenning niveau 1. De toegang zelf (autorisatie) is vastgelegd binnen het OndernemingsDossier.

Op dit moment staat er nog relatief weinig gevoelige informatie in het ondernemingsdossier. De informatie die momenteel in een ondernemingsdossier wordt klaargezet voor overheden is weliswaar niet zeer gevoelig, maar sommige informatie kan wel concurrentiegevoelig zijn. Bovendien is de imagoschade voor OndernemingsDossier en de Minister van EL&I aanzienlijk als bedrijfsinformatie uit een van de ondernemingsdossiers lekt. Daarom wordt een eHerkenning niveau 2 vereist op het gebied van vertrouwelijkheid. Problemen met het OndernemingsDossier kunnen weerslag hebben op de Minister van EL&I als politiek verantwoordelijke en als faciliteerder en stimulator in de eerste fase van OndernemingsDossier. De beschikbaarheid is afhankelijk van de dienst waarvoor de informatie wordt klaargezet.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse aanwezig?
Er is een initiële risicoanalyse uitgevoerd en de opgeslagen gegevens zijn geclassificeerd naar vertrouwelijkheidsniveaus, zowel voor ondernemingsgegevens als persoonsgegevens. Hieruit blijkt dat voor de toegang tot het ondernemingsdossier minimaal authenticatieniveau 2 nodig is.

Veiligheid in het ontwerp geborgd?
Het thema veiligheid staat op de agenda en in het huidige ontwerp lijkt de veiligheid voldoende geborgd te zijn, hierbij zij opgemerkt dat de impact op dit moment laag is.
Onderzoekers hebben documenten ter plaatse kunnen inzien.

Veiligheid in de beheerfase geborgd?
Een integrale governance met duidelijke veiligheidsparagraaf voor de samenwerking tussen overheid en het bedrijfsleven is noodzakelijk voor verder groei van het ondernemingsdossier. Hierin moet bijvoorbeeld de vraag worden beantwoord wie een onderzoek mag uitvoeren naar en eisen stellen aan de veiligheid van een ondernemingsdossier. De verantwoordelijkheid tussen beleidsopdrachtgever en private uitvoeringsorganisaties moeten expliciet worden gemaakt.

Risico's voldoende afgedekt?
Het ondernemingsdossier lijkt in dit stadium afdoende veilig.

Is de feitelijke werking van de elektronische dienst veilig?
De uitvoerders van het Ondernemersdossier lijken veiligheid zeer serieus te nemen, gezien de vorderingen die op het gebied van beheer en beveiliging gemaakt zijn in deze eerste fase.

Oordeel:
In het huidige beginstadium lijkt het OndernemingsDossier veilig, zoals uitgevoerd onder de verantwoordelijkheid van de initiatiefnemende branches. Een integrale governance met duidelijke veiligheidsparagraaf voor de samenwerking tussen overheid en het bedrijfsleven is noodzakelijk voor verder groei van het ondernemingsdossier. Hierin moet bijvoorbeeld de vraag worden beantwoord wie onderzoek mag uitvoeren naar en eisen moet stellen aan de veiligheid van een ondernemingsdossier.

Aanbevelingen:

- Voer een integrale governance in met expliciete aandacht voor veiligheid en duidelijk afgebakende en vastgelegde rollen voor de betrokken partijen, waaronder het ministerie van EL&I. Kijk hierbij ook naar de vraag of het Ministerie van EL&I onderzoek mag uitvoeren naar de veiligheid van het OndernemingsDossier bij de (private) partijen die verantwoordelijk zijn voor het ondernemingsdossier.
  Op dit moment zijn de koploperbranches bezig een serviceorganisatie in te richten voor beheer en doorontwikkeling. Het ligt voor de hand om de beveiligingsaspecten daar te beleggen.
- Voer eHerkenningsauthenticatie van niveau 2 aangevuld met machtiging van derden in zodra beschikbaar. Planning van eHerkenning is voorjaar van 2012.
- Vervang certificaten die gebruik maken van verouderde encryptie (SHA-1, Secure Hash Algoritme 1) door certificaten die gebruik maken van actuele encryptie (SHA-2, Secure Hash Algoritme 2).

B. Samenvatting SBR en eFactureren (inclusief Digipoort-PI)

Inleiding:
De diensten **Standaard Bedrijfsrapportage (SBR)** en **eFactureren** zijn in deze rapportage gecombineerd, omdat beide diensten voor hun belangrijkste functionaliteit, het uitwisselen van gegevens, afhankelijk zijn van dezelfde onderliggende infrastructuur, Digipoort-PI (Digipoort Proces Infrastructuur). Ook **Digipoort-PI** is in het onderzoek meegenomen.

De dienst **Standaard Bedrijfsrapportage (SBR)** bestaat uit een afsprakenstelsel voor het opstellen van bedrijfsrapportages en een faciliteit (Digipoort-PI) voor het versturen ervan.
De dienst **eFactureren** bestaat uit een afsprakenstelsel voor het opstellen van e-facturen en een faciliteit (Digipoort-PI) voor het versturen ervan.

Digipoort Proces Infrastructuur (Digipoort-PI) is een generieke voorziening voor het geautomatiseerd afwikkelen van informatie-uitwisselingsprocessen tussen bedrijven en overheden. Digipoort-PI maakt onderdeel uit van de infrastructuur van de e-overheid. Digipoort-PI zorgt voor het feitelijk uitwisselen van standaard bedrijfsrapportages en e-facturen. De operationele dienstverlening van Digipoort-PI komt tot stand onder de verantwoordelijkheid van Logius, een onderdeel van het Ministerie van BZK.

Risicoprofiel van de diensten:
De diensten SBR en eFactureren richten zich geheel op het veilig en betrouwbaar versturen van gegevens tussen bedrijven en overheden. Vanwege het hiervoor noodzakelijke vertrouwen, moet de veiligheid van de dienst zelf onberispelijk zijn. Dit vergt een zeer hoog beveiligingsniveau voor de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de diensten SBR en eFactureren, alsmede de onderliggende infrastructuur Digipoort-PI ernstig worden beschadigd.

De maximaal toegestane uitvalsduur is niet specifiek vastgelegd. Wel zijn er afspraken gemaakt over incidentafhandeling voor Digipoort-PI (melden, beoordelen en afhandelen van incidenten, inclusief maximale oplostijden).

Binnen Digipoort-PI worden persoonsgegevens verwerkt van risicoklasse 2[2] van Wbp (wet bescherming persoonsgegevens). Digipoort-PI heeft daarvoor de vereiste beveiligingsmaatregelen getroffen.

Naast de directe gevolgen door incidenten met betrekking tot SBR, eFactureren en Digipoort-PI, bestaan voor de deelnemende partijen - en met name voor de aanjagende partij, het Ministerie van EL&I - de reële mogelijkheid van imagoschade.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse(s) aanwezig?
Voor eFactureren en SBR zijn jaarlijks risicoanalyses op strategisch-tactisch niveau opgesteld. Voor Digipoort-PI zijn risicoanalyses gemaakt en deze worden goed bijgehouden, conform ISO 27001. Implementatie van de maatregelen wordt gemonitoord.

[2] Risicoklasse 2 betreft gevoelige persoonsgegevens, of grote hoeveelheden persoonsgegevens.

Veiligheid in het ontwerp geborgd?

Voor de afsprakenstelstels SBR en eFactureren is het eigenaarschap niet goed uitgekristalliseerd, maar de veiligheid is niet direct in het geding.

In het ontwerp speelt voor SBR en eFactureren veiligheid vooral een rol binnen Digipoort-PI. In het ontwerp van Digipoort-PI is veiligheid een belangrijk criterium geweest. Bij het ontwerp van de beheer- en beveiligingsprocessen is gebruik gemaakt van de beveiligingstandaard ISO 27001.

Veiligheid in de beheerfase geborgd?

De beheer- en beveiligingsprocessen op niveau Digipoort-PI zijn goed ingericht. Het huidige beveiligingsniveau is in overeenstemming met de gespecificeerde behoefte. De implementatie van nieuwe maatregelen naar aanleiding van wijzigingen uit de risicoanalyse wordt gemonitoord.

Risico's voldoende afgedekt?

De veiligheidsrisico's voor SBR en eFactureren vallen binnen Digipoort-PI op de geboden functionaliteit van de diensten na. De risico's voor Digipoort-PI lijken op basis van de verkregen informatie voldoende afgedekt te zijn.

Om imagoschade te beperken zijn er tussen Logius en Ministerie van EL&I afspraken gemaakt over woordvoering in geval van incidenten. Aangezien SBR en eFactureren stelsels zijn met meerdere aangesloten partijen kan er imagoschade ontstaan bij meerdere partijen (olievlek werking).

Is de feitelijke werking van de elektronische dienst veilig?

Worden de veiligheidsmaatregelen uitgevoerd zowel in de front- als de backoffice?

Alle uitvoering van beveiligingsmaatregelen zit in Digipoort-PI en bij de organisaties die op Digipoort-PI aangesloten zijn. De beveiliging van Digipoort-PI is goed aangepakt, hetgeen het vertrouwen geeft dat Digipoort-PI voldoende veilig is.

Wie controleert dit?

Logius en de onderliggende uitvoerders worden jaarlijks geaudit. Daarnaast worden regelmatig penetratietesten uitgevoerd.

Risico's voldoende afgedekt?

Het gekozen beveiligingsniveau is goed en de daarvoor benodigde maatregelen zijn geïmplementeerd. Dit betekent overigens niet dat er geen beveiligingsincident kan optreden, maar dat een goed beveiligingsniveau gekozen en geïmplementeerd is.

Oordeel:

Voor Digipoort-PI zijn veiligheid en beheer goed geregeld. SBR en eFactureren zijn afsprakenstelsels. Voor SBR en eFactureren is het eigenaarschap niet goed uitgekristalliseerd, maar de veiligheid is niet direct in het geding. De risico's voor SBR en eFactureren, voor zover deze betrekking hebben veiligheid, vallen binnen Digipoort-PI.

Aanbevelingen:

SBR en eFactureren:

- Geef aandacht aan het eigenaarschap van de diensten SBR en eFactureren, eventueel op delen van deze diensten.
- Voer ten behoeve van de voorgenomen stap van ingroei van de SBR-programma-"cel" binnen Logius een risicoanalyse per service over de ketenpartners uit in verband met de gewenste gegarandeerde dienstverlening.
- Oefen escalatietrajecten met stakeholders aan de hand van scenario's voor SBR en eFactureren en

leg dit vast in procedures. Zorg dat de verantwoordelijkheden en bevoegdheden duidelijk en vastgelegd zijn en dat hierover consensus bestaat.

Digipoort-PI:

- Inventariseer de verantwoordelijkheden en bevoegdheden m.b.t. SBR, eFactureren en Digipoort-PI, maak ze duidelijk en leg ze vast.
- Onderzoek in hoeverre het detecteren van hackers noodzakelijk of wenselijk is voor Digipoort-PI en implementeer daar zo nodig systemen voor.

C. Samenvatting eHerkenning

Inleiding:
eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij (overheids)dienstverleners. Bedrijven kunnen met hun eHerkenningsmiddel bij steeds meer (overheids)dienstverleners terecht en hebben niet meer bij iedere dienstverlener een ander authenticatiemiddel nodig. De dienstverlener op zijn beurt weet door eHerkenning precies met welk bedrijf hij zaken doet en of de betreffende persoon bevoegd is om namens dat bedrijf zaken te doen met de dienstverlener. Zelf hoeft de dienstverlener daarvoor geen eigen middelen voor identificatie en authenticatie uit te geven en te beheren.
De realisatie van eHerkenning gebeurt met een netwerk, waarin marktpartijen – de zogenaamde deelnemers – samenwerken om herkenningsdiensten te leveren. De ontwikkeling en het beheer van eHerkenning op stelselniveau worden in dit stadium nog uitgevoerd door een projectorganisatie en een Tijdelijke Beheerorganisatie (TBO).

Risicoprofiel van de dienst:
eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij (overheids)dienstverleners. Vanwege het hiervoor noodzakelijke vertrouwen, moet de veiligheid van de dienst zelf zeer goed op orde zijn. Dit stelt stringente eisen aan de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de dienst ernstig worden beschadigd.
De eisen aan de beschikbaarheid zijn beschreven in het afsprakenstelsel (Service Level). Iedere deelnemer moet gedurende de openstellingsduur (7:00 uur – 24:00 uur) voor 99,2% (gemeten per kalendermaand) gegarandeerd en volledig beschikbaar zijn. De maximaal toegestane uitvalsduur voor iedere deelnemer is vier uur binnen de openstellingsduur. Op stelselniveau kan de maximale uitvalsduur in principe hoger uitvallen omdat meerdere partijen in dezelfde keten achtereenvolgens maximaal vier uur uit zouden kunnen vallen.
Sommige partijen binnen de dienst eHerkenning verwerken persoonsgegevens. Daar waar persoonsgegevens verwerkt worden, is de Wbp (wet bescherming persoonsgegevens) van toepassing.
Naast de directe gevolgen door incidenten met betrekking tot eHerkenning, bestaat voor alle deelnemende partijen en met name voor de beleidsopdrachtgever en politiek verantwoordelijke, het Ministerie van EL&I, de reële mogelijkheid van imagoschade.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse(s) aanwezig? Op stelselniveau is een risicoanalyse opgesteld. Bovendien stelt elke deelnemer, inclusief de TBO, een risicoanalyse op voor het eigen deel van het eHerkenningsnetwerk. De risicoanalyses worden bijgehouden binnen het wijzigingsbeheer, maar zijn nog niet door een onafhankelijke partij gereviewd. Daardoor zijn er in de opzet mogelijk maatregelen over het hoofd gezien.

Veiligheid in het ontwerp geborgd? Veiligheid is een belangrijk criterium geweest in de ontwerpfase. Voor de ontwerp- en transitiefase is een tijdelijke stelselbeheerorganisatie, TBO, ontworpen en gerealiseerd. Deze voldoet voor de ontwerp- en transitiefase, maar niet voor de aanstaande definitieve beheerfase bij Logius.
De dienstverlening wordt geoperationaliseerd door de deelnemers (marktpartijen). Iedere deelnemer moet gecertificeerd zijn voor de beveiligingsstandaard ISO 27001 en het gemeenschappelijk normenkader beveiliging eHerkenning en daarmee aantoonbaar de eigen informatiebeveiliging op orde hebben. Aanvullende maatregelen, te weten stelselaudits en penetratietesten op het eHerkenningsnetwerk, worden ingezet om aan te tonen dat de

informatiebeveiliging ook op stelselniveau geborgd is.

Veiligheid in de beheerfase geborgd? De planning is erop gericht om per april 2012 het project eHerkenning af te ronden en over te dragen aan Logius. De huidige processen en procedures binnen TBO zijn voor de transitiefase bedoeld en niet voor de aanstaande definitieve beheerfase bij Logius. Het moet nog duidelijk gemaakt worden hoe de besturing-, beheer en beveiligingsprocessen op stelselniveau bij Logius zullen worden ingericht.

Deelnemers zullen ook in de aanstaande definitieve beheerfase gecertificeerd moeten zijn voor de beveiligingsstandaard ISO 27001 en het gemeenschappelijk normenkader beveiliging eHerkenning en daarmee aantoonbaar hun informatiebeveiliging op orde hebben. In aanvulling hierop zullen uitgebreide toetredings- en stelselaudits en penetratietesten voor het eHerkenningsnetwerk moeten worden gedaan.

Risico's voldoende afgedekt? Voor de huidige transitiefase zijn de belangrijke risico's in het ontwerp van eHerkenning afgedekt. Voor de aanstaande definitieve beheerfase moet nog duidelijk gemaakt worden hoe de besturing-, beheer en beveiligingsprocessen op stelselniveau bij Logius zullen worden ingericht. Tevens is extra aandacht nodig voor het voorbereiden van de overdracht naar Logius, het opstellen van een calamiteitenplan en het structureel inrichten van de governance voor het eHerkenningstelsel. Aanvullende zekerstelling is gewenst door het reviewen van de risicoanalyses en het bepalen of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn, het opstellen en gebruiken van gap-analyses en het vastleggen, reviewen en zo nodig aanpassen van het whitelist-proces.

Is de feitelijke werking van de elektronische dienst veilig?

Worden de veiligheidsmaatregelen uitgevoerd zowel in de front- als de backoffice? De ontworpen (deels tijdelijke) besturing-, beheer- en beveiligingsprocessen op stelselniveau en maatregelen uit het normenkader lijken op stelselniveau goed geïmplementeerd te zijn voor de huidige transitiefase.

Op deelnemerniveau wordt de uitvoering van de processen en maatregelen geborgd door de voor certificatie benodigde regelmatige audits. Een toetredingsaudit door een onafhankelijke auditor wordt nog niet uitgevoerd. Er worden regelmatig penetratietesten gedaan.

Er vindt beperkte monitoring plaats op de implementatie van wijzigingen en nieuwe maatregelen op deelnemer- en stelselniveau.

Stelselaudits zijn gepland, maar nog niet uitgevoerd. In het kader van dit onderzoek zijn aanvullende audits en penetratietesten bij de deelnemers niet nodig geacht, maar er moet wel vaart gemaakt worden met het uitvoeren van regelmatige stelselaudits.

Wie controleert dit? Toezicht op eHerkenning wordt momenteel uitgeoefend door het bestuur van eHerkenning, bestaande uit overheidsmarktpartijen en dienstaanbieders in het stelsel, ICTU en het Ministerie van EL&I. Het bestuur kan voor haar controlerende taak gebruik maken van de bevindingen uit de uitgevoerde audits en penetratietesten.

Risico's voldoende afgedekt? De beperkte monitoring van de implementatie van wijzigingen en nieuwe maatregelen op deelnemer- en stelselniveau en het ontbreken van uitgebreide toetredings- en stelselaudits kan leiden tot incidenten op het gebied van veiligheid.

Voor de borging van de veiligheid op termijn is het nodig om het implementeren van wijzigingen en nieuwe maatregelen effectief te monitoren en regelmatig een uitgebreide stelselaudit uit te voeren in opdracht van de beleidsopdrachtgever van eHerkenning.

Oordeel: Het ontwerp van de besturing-, beheer- en beveiligingsprocessen op stelselniveau is deels tijdelijk, maar voor de transitiefase voldoende veilig, zij het niet overtuigend. Aanvullende zekerstelling is gewenst, met name door onafhankelijke review van de risicoanalyses en het bepalen of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn. Daarnaast zou er vaart gemaakt moeten worden met de transitie naar de definitieve beheerfase bij Logius.

De ontworpen (deels tijdelijke) processen en de maatregelen uit het normenkader lijken op deelnemer- en stelselniveau goed geïmplementeerd te zijn, maar er vindt onvoldoende monitoring plaats op het implementeren van wijzigingen en nieuwe maatregelen. Dit kan leiden tot incidenten op het gebied van veiligheid.
Voor de borging van de veiligheid op termijn is het nodig om het ontwerp van de processen op stelselniveau te verbeteren, het implementeren van wijzigingen en nieuwe maatregelen effectief te monitoren en regelmatig een uitgebreide stelselaudit uit te voeren in opdracht van de eigenaar van eHerkenning.

Aanbevelingen:

- Richt de governance voor het eHerkenningstelsel structureel in en stem af met Logius.
- Zet vaart achter de voorbereidingen voor de overdracht aan Logius.
- Inventariseer de mogelijk maatregelen om imagoschade te voorkomen als incidenten m.b.t. eHerkenning optreden.
- Review de stelselrisicoanalyses en de risicoanalyse voor TBO en bepaal of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn.
- Stel op stelselniveau gap-analyses op en gebruik deze ook.
- Stel op stelselniveau een calamiteitenplan op.
- Stel de afspraken met betrekking tot audit zodanig bij dat de toetredingsaudits uniform, met dezelfde scope en diepte, uitgevoerd worden.
- Regel dat iedere stelsel- en toetredingsaudit een echte audit is en zich niet beperkt tot een review van bestaande auditrapporten. Bovendien moet de stelselaudit een inhoudelijke toetsing omvatten van de risicoanalyses en de gap-analyses.
- Voer regelmatig een stelselaudit uit. De stelselaudit moet in opdracht van de beleidsopdrachtgever, het ministerie van EL&I, uitgevoerd worden.
- Investeer niet in een eigen penetratietesttool, maar geef voorrang aan het verplicht invoeren van aanvullende stelselbrede beveiligingsmaatregelen bij de deelnemers.
- Leg het wijzigingsbeheer voor de whitelist vast, evalueer dit en pas het zo nodig aan.
- Voorkom dat verlopen certificaten te lang worden gebruikt door een redelijke termijn voor vervanging van certificaten te stellen.

D. Samenvatting Antwoordvoorbedrijven inclusief Ondernemersplatform en Open Data

Inleiding: Antwoordvoorbedrijven inclusief Ondernemersplatform en Open Data is een informatieve website die ondernemers wegwijs maakt door de grote hoeveelheid van informatie van de overheid.
Risicoprofiel van de dienst: Antwoordvoorbedrijven is een informatieve website met publieke informatie voor ondernemers.Antwoordvoorbedrijven bevat en verwerkt geen gevoelige gegevens of persoonsgegevens en heeft geen rol in de afhandeling van transacties van en met de overheid. Als de site enkele dagen tot een week niet beschikbaar is, is de impact laag. Hoewel er geen bijzondere eisen gesteld worden aan de veiligheid van de gepresenteerde gegevens, is het wenselijk dat de integriteit van de gegevens geborgd is.
Is het ontwerp van de elektronische dienst veilig? **Risicoanalyse(s) aanwezig?** TNO heeft in maart 2011 een risicoanalyse uitgevoerd. Hierin wordt geconcludeerd dat de onbeschikbaarheid van de site geen grote impact heeft. Destijds was de aanbeveling om Berichtenbox benaderbaar te maken als Antwoordvoorbedrijven niet beschikbaar is. Geïnterviewden gaven aan dat dit inmiddels een eis is en geregeld is. Verder worden nog mogelijke risico's op basis van softwarefouten benoemd. Na review van de softwarecode en het herstellen van de gevonden fouten is dit opgelost. Het vinden en herstellen van toekomstige fouten is nog niet procesmatig geborgd.
Is de feitelijke werking van de elektronische dienst veilig? Antwoordvoorbedrijven is een eenvoudige website. Regelmatige penetratietesten van de website geven aan dat het gerealiseerde beveiligingsniveau voldoende is. Bovendien wordt daarmee ook het beveiligingsniveau in de toekomst voldoende getoetst. Gezien het lage beveiligingsniveau dat nodig is voor Antwoordvoorbedrijven is geen verder onderzoek gedaan naar de beheer- en beveiligingsprocessen achter de beveiligingsmaatregelen.
Oordeel: Antwoordvoorbedrijven inclusief Ondernemersplatform en Open Data heeft voldoende aandacht voor veiligheid in de vorm van testen, ontwerpen en Threat and Vulnerability Analysis (TVA's).
Aanbevelingen: • Houdt veiligheid goed op de agenda van Antwoordvoorbedrijven. • Het Ondernemersplatform is een portal omgeving binnen Antwoordvoorbedrijven die in ontwikkeling is en in bètaversie beschikbaar. Het ontwerp van de veiligheid ziet er goed uit. Nieuwe toepassingen van derden worden ontsloten. Aanbevolen wordt deze toepassingen te testen.

E. Samenvatting Berichtenbox

Inleiding:
De Berichtenbox voor Bedrijven (BBvB) maakt organisatorisch onderdeel uit van Antwoordvoorbedrijven maar is in dit onderzoek apart behandeld. BBvB is ingericht om te voldoen aan de Europese Dienstenrichtlijn en de daaruit voortvloeiende Nederlandse Dienstenwet. Via BBvB kunnen bedrijven op een betrouwbare manier communiceren met de overheid voor zaken die onder de Dienstenwet vallen. BBvB valt onder verantwoordelijkheid van het Ministerie van EL&I. Functioneel beheer ligt bij Agenschap NL (AGNL). Het operationeel beheer is uitbesteed aan de bedrijven Ordina (o.a. regietaak), Centric/NXS en Anoigo. Er wordt op beleidsniveau nagedacht over een samengaan van de Berichtenbox voor Bedrijven met die voor burgers.

Risicoprofiel van de dienst: BBvB is bedoeld voor betrouwbare communicatie met de overheid. BBvB stelt hoge eisen op het gebied van vertrouwelijkheid en integriteit en middelmatige eisen waar het gaat om beschikbaarheid. Voor de dienst is bepaald dat de maximaal toegestane (aaneengesloten) uitvalsduur 2-3 dagen is.
Naast de directe gevolgen door incidenten met betrekking tot BBvB, bestaat voor alle deelnemende partijen en met name voor de 'eigenaar', het Ministerie van EL&I, de reële mogelijkheid van imagoschade.
De berichtenbox wordt nog zeer weinig gebruikt door bedrijven.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse aanwezig?
Eind 2010 – begin 2011 is een risicoanalyse op functioneel niveau uitgevoerd.

Veiligheid in het ontwerp geborgd?
Bij het ontwerp is uitgegaan van het beperken van de beveiligingsrisico's die gedefinieerd zijn in de standaard "Open Web Application Security Project". Er heeft een review van de softwarecode plaatsgevonden in 2010 die heeft geleid tot aanpassingen in de software. De risicoanalyse en de informatiebeveiligingsplannen worden niet goed bijgehouden. Er is nog geen gap-analyse opgesteld om bij te houden in hoeverre de maatregelen uit de beveiligingsplannen geïmplementeerd zijn. De beveiligingsplannen bevatten geen calamiteitenparagraaf.

Veiligheid in de beheerfase geborgd?
Met de operationeel beheerders zijn afspraken vastgelegd over incident-, probleem- en wijzigingsbeheer.

Risico's voldoende afgedekt?
De besturings-, beheer en beveiligingsprocessen zijn niet voldoende uitgewerkt. Hierdoor kunnen noodzakelijke beveiligingsmaatregelen over het hoofd gezien worden.

Is de feitelijke werking van de elektronische dienst veilig?

Worden de veiligheidsmaatregelen uitgevoerd zowel in de front- als de backoffice?
De belangrijkste beheerprocessen zijn op afsprakenniveau ingericht, maar door het ontbreken van audits is er geen duidelijkheid over de kwaliteit en het naleven van de procedures en beveiligingsmaatregelen.

Wie controleert dit?
Er hebben tot nog toe geen audits plaatsgevonden. Jaarlijks wordt een penetratietest gedaan door een externe partij.

Risico's voldoende afgedekt?
Er is de nodige aandacht geweest voor technische beveiligingsmaatregelen als *code reviews* en penetratietesten en het implementeren van de daaruit voortvloeiende verbeteringen; acties die op uitvoeringsniveau in deze situatie belangrijk bijdragen tot de veiligheid van de dienst nu.

Op dit moment is niet duidelijk of beoogde beveiligingsmaatregelen door de leveranciers in de praktijk uitgevoerd en nageleefd worden.

Oordeel:

- Voor nu is de berichtenbox technisch veilig. Op uitvoeringsniveau zijn acties (*code reviews*[3] en penetratietesten) uitgevoerd en opgevolgd om de veiligheid te bevorderen. Echter het ontwerp van de de besturing-, beheer en beveiligingsprocessen is niet voldoende uitgewerkt waardoor de veiligheid niet structureel is geborgd. Structurele aandacht voor de veiligheid dient te worden geborgd nu duidelijk is dat de Berichtenbox in elk geval in 2012 operationeel blijft. Doordat het ontwerp van de besturing-, beheer en beveiligingsprocessen niet voldoende is uitgewerkt zijn mogelijk noodzakelijke beveiligingsmaatregelen over het hoofd gezien. De implementatie van de processen en maatregelen uit het ontwerp is nog niet getoetst door middel van een audit. Daardoor is het onduidelijk in hoeverre de implementatie is afgerond. De mogelijke tekortkomingen in het ontwerp van de besturing-, beheer- en beveiligingsprocessen en het ontbreken van regelmatige audits in opdracht van de eigenaar van de dienst dienen met spoed te worden opgepakt om de veiligheid van deze dienst op korte termijn al sterk te verbeteren en te borgen.

Aanbevelingen:

- Breng de besturings-, beheer en beveiligingsprocessen op orde nu duidelijk is dat BBvB in 2012 nog bij Agentschap NL blijft.
- Richt periodieke audits in onder verwantwoordelijkheid van EL&I om de kwaliteit en naleving van procedures en beveiligingsmaatregelen te beoordelen die ook de applicatie- en technisch beheerders meenemen in het onderzoek. Zorg dat deze audit zich niet beperkt tot een review van bestaande auditrapporten van de applicatie- en technisch beheerders. Zorg dat de audits een inhoudelijke toetsing omvatten van de risico- en gap-analyses.
- Richt processen in om de risicoanalyse en het beveiligingsplan periodiek te updaten en een gap-analyse uit te voeren.Maak vaart met het laten opstellen van een calamiteitenplan.

[3] Code reviews: systematisch onderzoek naar broncode van software programma's

1 INLEIDING

Dit document beschrijft de uitkomst van een onderzoek dat in opdracht van het Ministerie van Economische Zaken, Landbouw en Innovatie (in het vervolg afgekort tot Ministerie van EL&I) is uitgevoerd door Collis en HEC ten aanzien van de veiligheid van de diensten uit de Digitale Agenda.nl.

Het Ministerie van EL&I is verantwoordelijk voor de Digitale Agenda en vanuit die optiek opdrachtgever voor het onderzoek.

Dit onderzoek is vrijdag 28 oktober 2011 gestart met een kick off met de opdrachtgever. Vrijdag 18 november 2011 is de rapportage in eerste concept opgeleverd en 5 december 2011 het definitieve concept. Het onderzoek heeft geleid tot verschillende conclusies en adviezen met betrekking tot de aan het onderzoek onderworpen diensten uit de Digitale Agenda.nl. Dit rapport beschrijft alle bevindingen van het onderzoek en geeft een oordeel over de beveiliging van de diensten en aanbevelingen voor het veiliger maken ervan.

1.1 Doelgroep

Deze rapportage is primair geschreven voor de opdrachtgever,de Directeur Regeldruk & ICT-beleid, alsmede de dossierhouders van de verschillende diensten. Daarnaast is dit rapport geschreven om input te leveren voor de Digitale Implementatieagenda van de Minister van Economische Zaken, Landbouw en Innovatie die begin december 2011 aan de Tweede Kamer wordt aangeboden.

1.2 Leeswijzer bij dit document

Dit document is als volgt samengesteld. Hoofdstuk 2 bevat de details met betrekking tot de onderzoeksopdracht van het Ministerie van EL&I aan Collis en HEC. In hoofdstuk 3 wordt het gekozen beoordelingskader beschreven. Vervolgens worden in hoofdstuk 4 de betrokken diensten aan de hand van dit beoordelingskader geëvalueerd. Ieder evaluatie van een dienst begint met een detailbeschrijving die bestaat uit een korte beschrijving van de dienst, het risicoprofiel van de dienst, de bevindingen van het onderzoek, het oordeel van de onderzoekers over de dienst en de aanbevelingen. Aan het eind van de beschrijving per dienst volgt een samenvatting van de bevindingen en de beoordeling van de dienst. In hoofdstuk 5 worden de overkoepelende conclusies van dit onderzoek beschreven.

2 OPDRACHT

2.1 Kader van de opdracht

Een Nederland dat vergrijst en moet concurreren in een open wereldeconomie, kan drie dingen doen: harder werken, langer werken en slimmer werken. De Digitale Agenda.nl focust op het laatste. Hoe kan ICT slim worden ingezet voor groei en welvaart? Welke randvoorwaarden zijn daarvoor nodig? Een geslaagde uitvoering van deze agenda voor de periode 2011 – 2015 geeft een krachtige impuls aan innovatie en economische groei. Een belangrijke randvoorwaarde voor het inzetten van ICT als stimulans voor groei en welvaart is de veiligheid en daarmee betrouwbaarheid van ICT.

De overheid en ICT raken steeds meer afhankelijk van elkaar. Verschillende uitvoeringsorganisaties werken samen. Ook is op dit moment de tendens dat generieke overheidsvoorzieningen in het Burger en Bedrijven domein vanuit één kader worden ontwikkeld. Dit betekent dat een falen in beveiliging van ICT direct invloed heeft op het functioneren van de dienstverlening van de overheid aan bedrijven en burgers.

De onveilige DigiNotar certificaten resulteerden in het weekend van 2 september 2011 tot 300 onbetrouwbare sites. De Tweede Kamer kwalificeerde dit als een digitale ramp. DigiNotar was de ultieme 'wake up call'.
De Tweede Kamer eist veel beter toezicht op ICT-projecten en de beveiliging van overheidsdiensten.

Tijdens het Algemeen Overleg met de Tweede Kamer van 15 september 2011 is in dit licht door de minister van Economische Zaken, Landbouw en Innovatie aangekondigd de Tweede Kamer te informeren over de veiligheid van diensten genoemd in de Digitale Agenda.nl [DigitaleAgenda]. Ditzelfde onderzoek was reeds eerder aangekondigd door de ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Veiligheid & Justitie (V&J), in het kader van de reactie op het DigiNotar-incident [Kamerbrief]. Het aangekondigde onderzoek valt in twee delen uiteen:

1. Het Ministerie van EL&I en het Ministerie van BZK doen gezamenlijk onderzoek naar het stelsel van en toezicht op gekwalificeerde certificaten.
2. Het Ministerie van EL&I voert onderzoek uit naar de processen die erop gericht zijn de veiligheid van de diensten van de Digitale Agenda.nl te garanderen.

Het tweede deel van dit onderzoek is door het Ministerie van EL&I uitgezet in de markt en is aan Collis en HEC gegund.

2.2 Opdracht en werkwijze

2.2.1 Opdracht

Het Ministerie van EL&I formuleert in haar opdracht [Opdracht] twee hoofdvragen, ieder met enkele deelvragen:

A. Is het ontwerp (inrichting, proces en beheer) van de elektronische overheidsdiensten die beschreven zijn in de Digitale Agenda.nl veilig?
   1. Is er een risicoanalyse gemaakt?
   2. Welke maatregelen zijn er in het ontwerp van de diensten genomen om veiligheid te borgen?
   3. Welke maatregelen zijn of worden in de beheerfase van de diensten genomen om de veiligheid te borgen?
   4. Dekken de maatregelen de risico's voldoende af, c.q. is de risicoanalyse betrouwbaar?

B. Is de feitelijke werking van de diensten veilig?
   1. Worden de maatregelen in het ontwerp en de beheerfase van de diensten in de praktijk uitgevoerd door betrokken stakeholders en zowel in de front- als de backoffice (voor zover de dienst reeds operationeel is) en wie controleert dit?
   2. Dekken de maatregelen de risico's voldoende af, c.q. is de risicoanalyse betrouwbaar, c.q. vragen operationele tekortkomingen om aanvullende maatregelen?

Deze vragen moeten in principe worden beantwoord voor negen diensten uit de Digitale Agenda.nl, te weten:

- Regelhulp
- OndernemingsDossier
- Standaard Bedrijfsrapportage (SBR)
- eFactureren
- eHerkenning
- Antwoordvoorbedrijven
- Ondernemersplatform (met name Digitaal Ondernemersplein)
- Open Data
- Berichtenbox

Nadat bleek dat er nog geen ontwerp of werkend systeem "Regelhulp voor bedrijven" bestaat, is in overleg met de opdrachtgever besloten dat de veiligheidsvraag voor deze dienst nog niet relevant is en dat deze dienst verder buiten de scope van het onderzoek blijft.

Het onderzoek richt zich op een combinatie van bestuurlijke en technische factoren. Er is expliciet gekozen om dit onderzoek in beperkte tijd te laten uitvoeren. Vanwege de korte doorlooptijd zijn de diensten parallel onderzocht. Uitgangspunten bij het onderzoek zijn:

- De opdracht invullen als een onderzoek van drie weken, waarbij de werkwijze van een audit gevolgd wordt.
- De opdrachtgever heeft verzocht op 18 november 2011 het eertse concept eindrapport op te leveren, en een definitief conceptrapport op 5 december 2011.
- Dat gegeven de doorlooptijd van het onderzoek een kritische selectie moet worden gemaakt van te interviewen personen, aantal interviews, alsmede het doen van locale inspecties.

2.2.2 Werkwijze

Tijdens de kick-off van het project op 28 oktober 2011 zijn de aanpak en de verwachtingen over de op te leveren producten doorgesproken. Verder is het mandaat voor het onderzoek besproken en de lijst met contactpersonen verstrekt. Na de kick-off is een verzoek tot het aanleveren van documenten zoals opgenomen in Appendix 1 verstuurd naar de contactpersonen van de verschillende diensten.

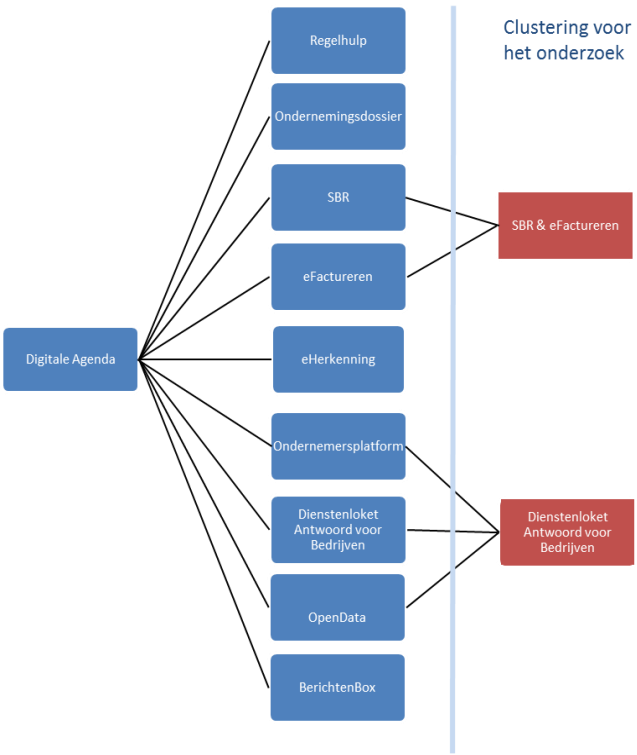
Daarna zijn de onderstaande stappen doorlopen:

1. Allereerst is het framework voor het evalueren van de veiligheid van de diensten vastgesteld. Dit framework is gedeeld met de opdrachtgever.
2. Vervolgens is een vragenlijst opgesteld die aan de diensten is voorgelegd als middel om informatie te verzamelen. Deze vragenlijst is aan de opdrachtgever aangeboden voor commentaar. De vragenlijst is opgenomen in Appendix 4.
3. Een tweede informatiebron vormden de ontwerp- en beheerdocumenten die de verschillende diensten hebben opgesteld. Hierop heeft een documentstudie plaats gevonden.
4. Verder zijn in verschillende stadia van het onderzoek interviews met de contactpersonen van de diensten gehouden. Interviewverslagen zijn aan de geïnterviewden voorgelegd om feitelijke onjuistheden te corrigeren.
5. Uit deze informatie is een risicoprofiel van de dienst gedestilleerd en afgestemd met de geïnterviewden van de betreffende dienst. Vervolgens zijn bevindingen ten aanzien van de veiligheid van de dienst geformuleerd.
6. Op basis van bovenstaande heeft – indien dit naar het oordeel van het onderzoeksteam waarde toevoegde aan de onderzoeksresultaten – lokale inspectie plaatsgevonden. Dat was het geval als op basis van de interviews en documentatie de veiligheidsstatus van een dienst niet goed vastgesteld kon worden. Per dienst is vervolgens een oordeel over de beveiliging opgesteld en aanbevelingen om de beveiliging te verbeteren.
7. Per dienst is wederhoor toegepast na het eerste conceptrapport (18 november 2011)
8. De bevindingen, conclusies en aanbevelingen zijn beschreven in dit rapport.

Een lijst van ontvangen documentatie en van gevoerde interviews is als appendix 3 toegevoegd aan dit document.

Clustering van diensten
In de loop van het onderzoek bleek dat enkele diensten zoveel raakvlakken hadden dat het logischer was om ze te clusteren en gezamenlijk te beoordelen.

De hiernaast weergegeven samenvoeging is gehanteerd.



3 RISICO- EN BEOORDELINGSKADER

Brondocumenten
Het framework waarbinnen de beoordeling heeft plaatsgevonden, is opgebouwd uit de standaarden die binnen de Nederlandse overheid van toepassing zijn. Daarbij is door ons een voorselectie gedaan op relevantie. Het betreft standaarden op het gebied van:

1. Architectuur.
2. Informatiearchitectuur.
3. Bedrijfsarchitectuur.
4. Beheer.
5. Informatiebeveiliging.
6. Ministeriebrede informatiebeveiliging (EL&I).

Voor een uitgebreide beschrijving wordt verwezen naar Appendix 2.

Daarnaast is het STORK framework gebruikt [STORK]. STORK is een Europees project geweest waarbij onder andere betrouwbaarheidsniveaus voor authenticatie zijn vastgelegd op vier niveaus, met als doel om op Europese schaal authenticatie vergelijkbaar en uitwisselbaar te maken.

Risico- en Beoordelingskader
De onderzoekers hebben op basis van de brondocumenten en de vraag van Ministerie van EL&I bepaald dat de diensten moeten worden onderzocht op:

- Eigenaarschap, toezicht en beheer, op meerdere verantwoordelijkheidsniveau's.
- Eindverantwoordelijkheid voor informatiebeveiliging van de dienst, op meerdere verantwoordelijkheidsniveau's.
- Vaststelling op van toepassing zijnde wet en regelgeving (o.a. vaststelling Wbp risicoklasse van de dienst).
- Vaststelling welk STORK niveau authenticatie nodig is om gebruik te maken van de dienst.
- In het ontwerp en beheersfase van de dienst:
    - Aanwezigheid en actualiteit van risicoanalyses, inclusief vervolgprocessen om risico's te beheersen, op meerdere verantwoordelijkheidsniveau's. Is er acceptatie van de restrisico's op deze verantwoordelijkheidsniveau's.
    - Opdrachtverlening en afstemming van beveiligingseisen tussen opdrachtnemer en opdrachtgever als er meerdere partijen zijn?
    - Inrichting van beheerprocessen, met name incident-, configuratie- en wijzigingsbeheer.
    - Maatregelen in het ontwerp van de diensten om veiligheid te borgen.
    - Maatregelen in het ontwerp voor het dichten van achterdeuren.
    - Maatregelen in de beheerfase van de diensten om veiligheid te borgen.
    - Maatregelen in de beheerfase voor het dichten van achterdeuren.
    - Aangebrachte scheiding van productieomgeving met ontwikkel-, test- en acceptatieomgeving.
    - Aanwezigheid toegangsbeleid en –procedures tot beheers(systemen).
    - Gemaakte keuzes ten aanzien van beveiligingsmechanismen en certificaten.
- De feitelijke werking van de dienst:
    - Borging van de ontworpen maatregelen.
    - Borging van de maatregelen in de beheersfase.

- Audits en penetratietesten.
- Aangetroffen beveiligingsmechanismen en certificaten.
- Aanwezigheid en actualiteit van risicoanalyses, inclusief vervolgprocessen om risico's te beheersen, op meerdere verantwoordelijkheidsniveau's.

Gebaseerd op het bovenstaande is een lijst met 37 vragen opgesteld, aan de hand waarvan betrokkenen van de verschillende diensten zijn bevraagd. De vragenlijst is opgenomen in Appendix 4.

Daarnaast is gebruik gemaakt van de ervaring van de onderzoekers bij het beoordelen van de beveiliging om daar door te vragen waar nodig.

Opstellen risicoprofielen
Van alle diensten is een risicoprofiel van de dienst gemaakt met betrekking tot veiligheid. Veiligheidsaspecten die hierbij meegenomen zijn beschikbaarheid, (data)integriteit, vertrouwelijkheid en maximale toegestane uitvalduur.

Veiligheidsaspect	Vereist beveiligingsniveau (in huidige beginstadium)
Beschikbaarheid	Laag / Middelmatig / Hoog
Integriteit	Laag / Middelmatig / Hoog
Vertrouwelijkheid	Laag / Middelmatig / Hoog
Maximale Toegestane uitvalduur (MTU)	Uren / Dagen

Op basis van het opgemaakte risicoprofiel is de diepte van het onderzoek bepaald. Diensten die met bekende en vaak toegepaste middelen en technieken te realiseren zijn, zoals het aanbieden van informatiepagina's op een website, zijn minder risicovol dan een dienst waaraan hogere (en bijzondere) beveiligingseisen zijn gesteld. Daarnaast is gebruik gemaakt van de ervaring van de onderzoekers bij het beoordelen van de beveiliging.

Restrisico's
Bij iedere dienst is een restrisico aanwezig. Het is namelijk niet haalbaar en niet betaalbaar om de risico's voor de dienst tot nul te reduceren. De eigenaar van de dienst bepaalt welke kosten voor het beveiligen van de dienst nog redelijk zijn, en daarmee welk restrisico acceptabel is. Dit betekent echter dat bij het volledig en correct implementeren en uitvoeren van alle beoogde beveiligingsmaatregelen, toch een beveiligingsincident op kan treden. Het restrisico voor de dienst moet bewust geaccepteerd en vastgelegd worden door de eigenaar van de dienst.

Audits versus (staats)toezicht
In het rapport wordt het begrip 'audit' veel gebruikt. Een audit is een beoordeling door een onafhankelijk deskundige partij tegen een door de eigenaar van de dienst vastgestelde norm. Een audit is een aanvulling op het kwaliteitssysteem van een organisatie die een elektronische dienst levert en/of beheert. Een audit levert verbeterpunten op en bij het voldoen aan de normen kan de organisatie dit door middel van een certificaat aantonen aan derden. Auditorganisaties en certificeringinstellingen zijn gehouden aan kwaliteitsnormen en beroepscodes. Staatstoezicht geschiedt op basis van wettelijke normen en bevoegdheden door een onafhankelijk toezichthouder of inspectie. De systematiek en het doel van een audit is wezenlijk anders dan die van staatstoezicht. Dit onderscheid is van belang bij het lezen van deze rapportage.

4 BEOORDELING PER DIENST

In onderstaand hoofdstuk volgt na enkele waarnemingen vooraf de rapportage per dienst of dienstencluster. De volgende opbouw aangehouden:

1. Korte beschrijving van de dienst, gebaseerd op de verstrekte informatie en publiek beschikbare informatie over deze dienst.
2. Risicoprofiel van de dienst, in het bijzonder het belang van de aspecten integriteit, vertrouwelijkheid en beschikbaarheid. Daarnaast speelt het privacybelang mee.
3. De uit het onderzoek voortkomende bevindingen.
4. Een oordeel over de dienst.
5. Aanbevelingen voor de dienst.
6. Samenvatting.

4.1 Enkele waarnemingen vooraf

Tijdens het onderzoek is gebleken dat de geïnterviewden sterk betrokken zijn bij de (ontwikkeling van de) betreffende diensten. Kwalitatief goede input werd gegeven – zowel in woord als in documentatie.

De informatie ten behoeve van het onderzoek kwam wat moeizaam op gang. Met name informatie over beleidsuitgangspunten, besluiten, aansturing en verantwoordelijkheden van betrokkenen zou vroeger in het onderzoeksproces behulpzaam zijn geweest.

Tijdens het onderzoek is voldoende snel gereageerd op vragen van de onderzoekers. Met betrekking tot de uitbreiding van het onderzoek naar de veiligheid van Digipoort-PI, als ondersteunende dienst voor SBR en eFactureren, is binnen korte tijd op directeurniveau overleg gevoerd en ingestemd.

Met betrekking tot de beveiliging van informatie merken de onderzoekers op dat documentatie die te omvangrijk was om via e-mail te versturen, aan de onderzoekers werd verstrekt via een informatieopslagvoorziening van een private (gratis) aanbieder. Bestanden die via deze voorziening worden gecommuniceerd, worden volgens de condities van de betreffende aanbieder beheerd. Hoewel de aanbieder van de voorziening volgens hun gebruikersvoorwaarden geen rechten op de informatie claimt en de informatie beschermt, conformeert de aanbieder zich aan wetgeving van USA. De onderzoekers zijn van mening dat bij het gebruik van een dergelijke voorziening de controle over de informatie feitelijk uit handen wordt gegeven. Daarom raden de onderzoekers het gebruik daarvan af.

Daarnaast is het de onderzoekers opgevallen dat in één geval het e-mailadres voor uitwisselen van informatie niet van een onderdeel van de Rijksoverheid is, maar een van een openbare private (gratis) aanbieder. De onderzoekers zijn van mening dat dit niet de bedoeling is. Informatie van/voor overheidsfunctionarissen dient van/naar een overheidsadres, of een adres van een voor de overheid werkende organisatie te worden gestuurd.

4.2 Regelhulp

4.2.1 Korte beschrijving

Op dit moment wordt er door Berenschot een onderzoek uitgevoerd naar de positionering van Regelhulp [Regelhulp]. De verwachte oplevering van dit onderzoek is februari 2012. Probleemstelling van dit onderzoek is: "*Wat zijn de succes- en faalfactoren voor een strategie voor de brede invoering van regelhulp en welke elementen en sturingsfilosofie zou deze moeten bevatten?*"

Tijdens het interview gaf EL&I aan dat op basis van dit onderzoek de meerwaarde van het concept Regelhulp wordt bepaald. Op basis hiervan wordt besloten of Regelhulp er komt. Onderdeel van het onderzoek is ook de vraag in hoeverre de overheid, dan wel de markt een rol heeft bij de ontwikkeling van regelhulp. Ook op termijn zal de rol van EL&I hoogstens een faciliterende zijn.
Dit traject bevindt zich momenteel dus nog in een inventariserende fase, waarbij zowel de behoefte aan als mogelijkheden tot brede invoering van Regelhulp in kaart wordt gebracht. Vragen over risicoanalyses, te kiezen authenticatieniveau en de te kiezen beveiligingsoplossing zijn nu nog niet aan de orde.

Regelhulp is buiten de scope van het onderzoek geplaatst. Na kennisneming van de documentatie bleek er nog geen ontwerp of werkend systeem "Regelhulp voor bedrijven" te bestaan. In overleg met de opdrachtgever is besloten dat de veiligheidsvraag nog niet relevant is.

4.2.2 Conclusie / aanbevelingen

We adviseren bij een toekomstige implementatie van "Regelhulp" dat de verantwoordelijke organisatie een risicoanalyse uitvoert op het gebied van veiligheid. De hieruit voortvloeiende maatregelen dienen te worden geborgen en gecontroleerd.

4.2.3 Samenvatting

Regelhulp is buiten de scope van het onderzoek geplaatst. Na kennisneming van de documentatie bleek er nog geen ontwerp of werkend systeem "Regelhulp voor bedrijven" te bestaan. In overleg met de opdrachtgever is besloten dat de veiligheidsvraag nog niet relevant is.

4.3 OndernemingsDossier

4.3.1 Korte beschrijving

Het OndernemingsDossier is een verzameling digitale dossiers van ondernemers die door ondernemingen zelf bij een centrale dienstverlener worden gerealiseerd volgens bepaalde standaarden. Een ondernemingsdossier stelt een onderneming in staat om bepaalde informatie uit de eigen bedrijfsvoering beschikbaar te stellen aan verschillende overheden, zodat er uiteindelijk één informatiebron is van het bedrijf voor verschillende overheden. De onderneming bepaalt zelf welke overheden toegang hebben tot haar ondernemingsdossier.

Brancheorganisaties, hun leden en overheden spreken met elkaar af hoe zij informatie willen uitwisselen en leggen dat vast in samenwerkingsovereenkomsten. Deze overeenkomsten leggen de basis om met de ondernemingsdossiers te kunnen werken. Zo worden bijvoorbeeld afspraken gemaakt over welke documenten in een ondernemingsdossier worden geplaatst, welke bevoegdheden de gemachtigde overheden hebben om deze documenten in te zien en hoe vaak er dan nog op locatie moet worden geïnspecteerd. De ondernemer legt vervolgens zijn relevante bedrijfsgegevens in het ondernemingsdossier vast en houdt deze zelf actueel. De onderneming machtigt vervolgens verschillende overheidsinstanties deze gegevens in te zien. Zo kunnen deze instanties steeds over actuele informatie beschikken en hoeft er minder op locatie geïnspecteerd te worden.

Het idee voor het OndernemingsDossier ontstond bij de brancheorganisatie NRK voor de Rubber- en Kunststofindustrie en in de Horecabranche. Daar verkenden ondernemers en overheden samen de mogelijkheden om de controle op het naleven van de regels makkelijker te maken.

Het OndernemingsDossier wordt om te beginnen ingevoerd bij drie koploperbranches, (horeca, recreatie en rubber- en kunststofindustrie). Gestart wordt met 46 bedrijven, 11 gemeenten, 2 provincies en 2 rijksinspecties (eind 2011).
Inmiddels zijn in drie brancheorganisaties (Horeca, Rubber- en Kunststofindustrie en Recreatie) ervaringen opgedaan met een voorloper van het OndernemingsDossier. Het Centrum voor Publieke Innovatie (CPI) is de beheerder van dit OndernemingsDossier, in opdracht van de betrokken brancheorganisaties. Het CPI geeft aan dat het OndernemingsDossier sinds oktober 2011 live is met zeven ondernemingsdossiers en een beperkt aantal overheidsinstanties die de gegevens mogen inzien. Volgens CPI is het de ambitie van de brancheorganisaties om eind 2012 ongeveer 5000 ondernemers aangesloten te hebben. Het OndernemingsDossier is dus in een beginstadium.

In de huidige opzet van het Ondernemingdossier is niet voorzien in een informatiestroom van de overheidsinstanties naar de ondernemingsdossiers. Hiervoor wordt vooralsnog gebruik gemaakt van de bestaande communicatiekanalen.

	OndernemingsDossier
Status	In beginstadium
Eigenaar	De brancheorganisaties Horeca, Rubber- en Kunststofindustrie en Recreatie zijn eigenaar van het systeem waarin OndernemingsDossier gerealiseerd is. Naar verwachting gaan meerdere brancheorganisaties hieraan meedoen. Iedere onderneming is eigenaar van zijn eigen ondernemingsdossier
Functioneel beheer	Brancheorganisaties/CPI

Applicatie beheer	CPI
Technisch beheer	CPI

4.3.2 Risicoprofiel

De veiligheidsaspecten van het OndernemingsDossier hebben voornamelijk te maken met de classificatie van de opgeslagen gegevens, het beschermen ervan en het organiseren van de toegang. Voor dat laatste kan het OndernemingsDossier gebruik maken van eHerkenning.

Op dit moment staat er nog relatief weinig gevoelige informatie is het ondernemingsdossier. De beschikbaarheid van het dossier is afhankelijk van de partijen waarvoor de informatie wordt klaargezet. In het algemeen staat er geen spoedeisende informatie in de ondernemingsdossiers. De eisen aan de beschikbaarheid zijn dan ook middelmatig. De dienst stelt hoge eisen aan de (data)integriteit. Er staat kwalitatieve informatie over de onderneming in het ondernemingsdossier. De meeste informatie die in een ondernemingsdossier wordt klaargezet voor overheden is weliswaar niet zeer gevoelig, maar sommige informatie kan concurrentiegevoelig zijn. Bovendien is de imagoschade voor OndernemingsDossier aanzienlijk als bedrijfsinformatie uit een van de ondernemingsdossiers lekt. Daarom wordt een hoog beveiligingsniveau vereist op het gebied van vertrouwelijkheid. Problemen met het OndernemingsDossier kunnen weerslag hebben op de Minister van EL&I als politiek verantwoordelijke en faciliteerder, stimulator in de eerste fase van OndernemingsDossier.

Veiligheidsaspect	**Vereist beveiligingsniveau (in huidige beginstadium)**
Beschikbaarheid	Middelmatig
Integriteit	Hoog
Vertrouwelijkheid	Hoog
Maximale Toegestane uitvalduur (MTU)	Hoog

4.3.3 Bevindingen

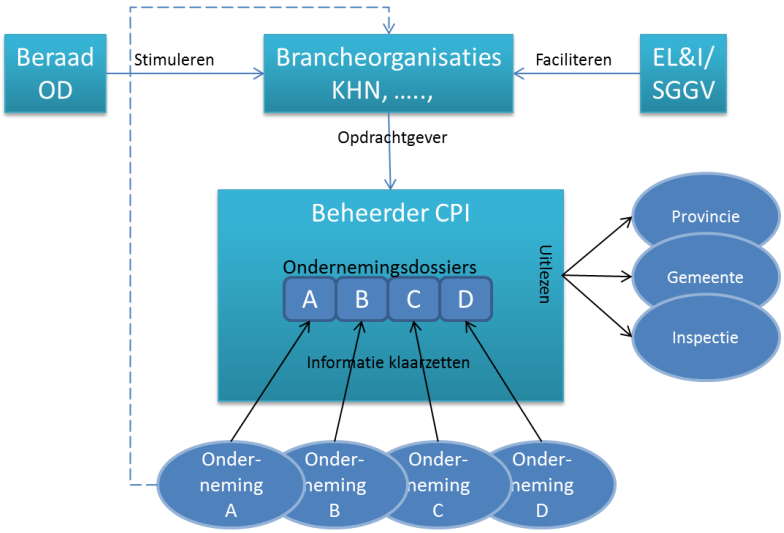
Algemeen
De eigenaren van de ondernemingsdossiers zijn de brancheverenigingen. De onderzoekers hebben contact gehad met de Horeca Brancheverenigingen om een indicatie te krijgen over de veiligheid van het Ondernemingsdossier en er is een interview gehouden met de beheerder CPI. Er heeft geen uitgebreid onderzoek plaatsgevonden naar de veiligheid van het OndernemingsDossier, wel zijn enkele veiligheidsdocumenten ter plaatse ingezien.

Het OndernemingsDossier staat in de Digitale Agenda.nl van het Ministerie van EL&I. Echter de realisatie en beveiliging ervan is belegd bij de initiatiefnemende branches. Het programma

SGGV[4]/OndernemingsDossier faciliteert de initiatiefnemende branches in opdracht van het Ministerie van EL&I. Concreet betekent dit dat brancheorganisaties en daarmee de ondernemingen in de branche primair verantwoordelijk zijn voor het specificeren en realiseren van onder meer de veiligheid van de ondernemingsdossiers.

Op dit moment zijn de koploperbranches bezig een service-organisatie in te richten voor beheer en doorontwikkeling. Het ligt voor de hand om de beveiligingsaspecten daar te beleggen.

In haar faciliterende rol ontwikkelt het ministerie de standaarden voor het OndernemingsDossier op basis van een algemene referentiearchitectuur, in afstemming met betrokken bedrijfsleven, overheidsorganisaties en ICT-marktpartijen. De standaarden die inmiddels ontwikkeld zijn, worden beheerd door het ministerie. In de faciliterende rol die het ministerie inneemt, zijn de branches gewezen op de mogelijke te nemen maatregelen, zoals audits en penetratietesten. De standaarden gaan dus ook over veiligheid. De verschillende brancheorganisaties moeten deze standaarden adopteren, aanvullen en voorschrijven aan hun leden. De onderzoekers hebben geen documentatie over governance voor OndernemingsDossier ontvangen. Op basis van de interviews is onderstaande schets opgesteld (figuur 1).



Figuur 1: schets integrale governance OndernemingsDossier

Sinds 14 september 2011 is een “Beraad OndernemingsDossier” ingesteld op bestuurlijk niveau. Het Beraad zorgt voor draagvlak. Het Beraad heeft een stimulerende taak en kan besluiten nemen ten aanzien van hun bestuurlijke-strategische rol, maar niet over daadwerkelijke invoering. Dat is aan de begreffende gemeenten en aansluitende overheidsorganisaties. Het Beraad heeft zichzelf nog geen concrete taak op het gebied van veiligheid gegeven.

[4] Het programma *Slim geregeld, goed verbonden (Sggv)* ondersteunt ketens van publieke en private partijen bij vermindering van de regeldruk voor het bedrijfsleven. Opdrachtgever is het ministerie van Economische Zaken, Landbouw en Innovatie

De opdrachtgever van de ondernemingdossiers zijn de brancheorganisaties namens de ondernemingen. In de nabije toekomst moet er een opdrachtgeversorgaan ontstaan bestaande uit meerdere brancheorganisaties.

Het beheer van het OndernemingsDossier is op dit moment belegd bij een marktpartij, namelijk CPI. De brancheorganisaties zijn in deze constructie opdrachtgever en eigenaar van het “systeem” OndernemingsDossier. De beheerorganisatie CPI is opdrachtnemer voor beheer van het OndernemingsDossier. De plannen zijn om in de toekomst een OndernemingsDossier Uitvoeringsorganisatie op te richten die meerdere branches bedient. Ook dit wordt een marktpartij.

Overheidsinstanties kunnen inzage krijgen in ondernemingsdossiers en de informatie daaruit gebruiken in hun primaire processen. Afspraken hierover, onder meer afspraken over veiligheid, worden geregeld via samenwerkingsovereenkomsten. De onderzoekers hebben geen samenwerkingsovereenkomsten ontvangen en kunnen hier geen uitspraak over doen. In de opdracht van de branches heeft CPI als beheerder een taak gebied veiligheid mee gekregen. Slordigheden van overheidsinstanties kunnen leiden tot beveiligingsissues. Strikt genomen valt dit buiten de scope van het OndernemingsDossier, maar dit kan ook zijn weerslag hebben op de Minister van EL&I als politiek verantwoordelijke en faciliteerder, stimulator en gebruiker van informatie uit het ondernemingsdossier .

Het Ministerie van EL&I heeft de onderzoekers verzocht informatie over het OndernemingsDossier te vergaren bij de brancheorganisatie Koninklijke Horeca Nederland en de OndernemingsDossierbeheerder het CPI. Deze private partij heeft ter plaatse relevante documenten ter inzage gegeven, maar stelt dat het onderzoek bij een private partij out of scope is. Op basis van deze ervaring lijkt het noodzakelijk om de rollen en verantwoordelijkheden in het kader van de veiligheid van het OndernemingsDossier te heroverwegen en expliciet te maken.

Uit documenten en een gesprek met CPI komt het volgende beeld over de beveiliging van het OndernemingsDossier naar voren:

- Er is een initiële risicoanalyse uitgevoerd en de opgeslagen gegevens zijn geclassificeerd naar vertrouwelijkheidsniveaus, zowel voor ondernemingsgegevens als persoonsgegevens. Hieruit blijkt dat authenticatieniveau 2 nodig is voor toegang tot het ondernemingsdossier.
- De toegang tot ondernemingsdossiers maakt momenteel gebruik van eHerkenning, niveau 1, met een aanvullende controle binnen het dossier.
- Een ondernemer kan te allen tijde zelf besluiten welke gebruiker toegang heeft tot welke gegevens.
- Het ondernemingsdossier laat voor externe partijen slechts raadplegen toe, geen invoer of wijziging van gegevens.
- Het beheer is ondergebracht in een extra beveiligde aparte applicatie en de ontwikkeling maakt gebruik van gescheiden OTAP omgevingen (Ontwikkel, Test, Acceptatie en Productieomgevingen plus en training omgeving).
- Penetratietesten zijn gepland, maar nog niet uitgevoerd vanwege het feit dat de dienst nog maar enkele weken geleverd wordt, dit is logisch gezien het beginstadium van de dienst.

CPI geeft aan dat het OndernemingsDossier behoefte heeft aan eHerkenning niveau 2, aangevuld met machtiging van derden. Niveau 1 wordt nu gebruikt. Daarom zijn nu aanvullende maatregelen nodig, namelijk extra toegangscontroles, om op een vergelijkbaar niveau te komen. In het tweede kwartaal van 2012 is gepland om over te gaan naar eHerkenning niveau 2. Op dat moment zal niveau 2 inclusief machtigingen en attributen in eHerkenning beschikbaar zijn.

Techniek
Tijdens de inzage van documenten ter plaatse bleek dat de gebruikte PKI-certificaten (Public Key Infrastructuur certificaten) wordt gebruik gemaakt van een verouderd cryptografisch algoritme, namelijk SHA-1 (Secure Hash Algoritme 1, internationale standaard, verouderd).

4.3.4 Oordeel

Algemeen
Het OndernemingsDossier is in een beginstadium. De rollen en bevoegdheden van het Ministerie van EL&I moeten geëxpliciteerd worden.

Beleid, standaarden, processen en procedures
De onderzoekers hebben documentonderzoek uitgevoerd. Er is weinig informatie over de ondernemingsdossiers beschikbaar gesteld en deze is ter plaatse ingezien. Het OndernemingsDossier lijkt op de beoogde wijze te kunnen werken, mits de governance in de nabije toekomst goed geregeld wordt.

Als er incidenten met betrekking tot OndernemingsDossier optreden kan er imagoschade ontstaan. Dit kan ook weerslag hebben op de Minister van EL&I als politiek verantwoordelijke en in de hoedanigheid van faciliteerder en stimulator. Het is nodig dat het Ministerie van EL&I haar rol expliciteert ten opzichte van de private partijen en de governance en beveiliging op korte termijn goed inricht.

Techniek
Ten aanzien van gebruikte certificaten blijkt dat bij CPI wordt gewerkt met certificaten die gebruik maken van een verouderd cryptografisch algoritme, namelijk SHA-1 (Secure Hash Algoritme 1, internationale standaard, verouderd).

4.3.5 Aanbevelingen

Algemeen
- Voer een integrale governance in met expliciete aandacht voor veiligheid en duidelijk afgebakende en vastgelegde rollen voor de betrokken partijen, waaronder het Ministerie van EL&I. Kijk hierbij ook naar de vraag wie onderzoek mag uitvoeren naar de veiligheid van het OndernemingsDossier. Aangezien het toezicht nog niet structureel is ingericht zou het “Beraad OndernemingsDossier” hiervoor een oplossing kunnen bieden.

Beleid, standaarden, processen en procedures
- Voer eHerkenningsauthenticatie van ten minste niveau 2 in, zodra dit beschikbaar is in het voorjaar van 2012.

Techniek
- Vervang PKI-certificaten die gebruik maken van SHA-1 door PKI-certificaten die gebruik maken van SHA-2 (Secure Hash Algoritme 2, actuele internationale standaard).

4.3.6 Samenvatting

Inleiding:
Het OndernemingsDossier is een initiatief en de verantwoordelijkheid van de initiatiefnemende branches. Het Ministerie van EL&I faciliteert de totstandkoming van het OndernemingsDossier en stelt door middel van algemene referentiearchitectuur standaarden voor. Op verzoek van de opdrachtgever zijn gesprekken gevoerd om een beeld van de veiligheid op te bouwen. Op basis hiervan is het onderzoek naar veiligheid gebaseerd.
Het OndernemingsDossier is in het beginstadium. Eind 2012 worden 5000 aangesloten ondernemers verwacht. Het OndernemingsDossier wordt om te beginnen ingevoerd bij drie koploperbranches, (horeca, recreatie en rubber- en kunststofindustrie). Gestart wordt met 46 bedrijven, 11 gemeenten, 2 provincies en 2 rijksinspecties (eind 2011). Overheden hebben(op basis van autorisatie en toestemming van de ondernemer) inzage in de kwalitatieve gegevens.

Risicoprofiel van de dienst:
De veiligheidsaspecten van het OndernemingsDossier hebben voornamelijk te maken met de classificatie van de opgeslagen gegevens, het beschermen ervan en het organiseren van de toegang voor ondernemers en overheidsorganisaties. Daartoe maakt het OndernemingsDossier voor identificatie en authenticatie van alle gebruikers nu gebruik van eHerkenning niveau 1. De toegang zelf (autorisatie) is vastgelegd binnen het OndernemingsDossier.

Op dit moment staat er nog relatief weinig gevoelige informatie in het ondernemingsdossier. De informatie die in een ondernemingsdossier wordt klaargezet voor overheden is weliswaar niet zeer gevoelig, maar sommige informatie kan concurrentiegevoelig zijn. Bovendien is de imagoschade voor OndernemingsDossier aanzienlijk als bedrijfsinformatie uit een van de ondernemingsdossiers lekt. Daarom wordt een hoog beveiligingsniveau vereist op het gebied van vertrouwelijkheid. Problemen met het OndernemingsDossier kunnen weerslag hebben op de overheid in de hoedanigheid van faciliteerder en stimulator in de eerste fase van OndernemingsDossier. De informatie die in een ondernemingsdossier wordt klaargezet voor overheden is weliswaar niet zeer gevoelig, maar sommige informatie kan concurrentiegevoelig zijn.
De beschikbaarheid is afhankelijk van de dienst waarvoor de informatie wordt klaargezet.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse aanwezig?
Er is een initiële risicoanalyse uitgevoerd en de opgeslagen gegevens zijn geclassificeerd naar vertrouwelijkheidsniveaus, zowel voor ondernemingsgegevens als persoonsgegevens.

Veiligheid in het ontwerp geborgd?
Het thema veiligheid staat op de agenda en in het huidige ontwerp lijkt de veiligheid voldoende geborgd te zijn, hierbij zij opgemerkt dat de impact op dit moment laag is.
Onderzoekers hebben documenten ter plaatse kunnen inzien.

Veiligheid in de beheerfase geborgd?
Een integrale governance met duidelijke veiligheidsparagraaf voor de samenwerking tussen overheid en het bedrijfsleven is noodzakelijk voor verder groei van het ondernemingsdossier. Hierin moet bijvoorbeeld de vraag worden beantwoord wie een onderzoek mag uitvoeren naar en eisen aan de veiligheid van een ondernemingsdossier.

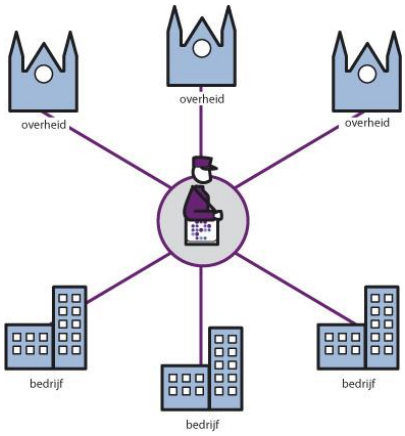
Risico's voldoende afgedekt?

Het ondernemingsdossier lijkt in dit stadium afdoende veilig.
Is de feitelijke werking van de elektronische dienst veilig? De uitvoerders lijken veiligheid zeer serieus te nemen, gezien de vorderingen die op het gebied van beheer en beveiliging gemaakt zijn in deze eerste fase.
Oordeel: In het huidige beginstadium lijkt het OndernemingsDossier veilig, zoals uitgevoerd onder de verantwoordelijkheid van de initiatiefnemende branches. Een integrale governance met duidelijke veiligheidsparagraaf voor de samenwerking tussen overheid en het bedrijfsleven is noodzakelijk voor verder groei van het ondernemingsdossier. Hierin moet bijvoorbeeld de vraag worden beantwoord wie een onderzoek mag uitvoeren naar en eisen stellen aan de veiligheid van een ondernemingsdossier.
Aanbevelingen: • Voer een integrale governance in met expliciete aandacht voor veiligheid en duidelijk afgebakende en vastgelegde rollen voor de betrokken partijen, waaronder het ministerie van EL&I. Kijk hierbij ook naar de vraag of het Ministerie van EL&I onderzoek mag uitvoeren naar de veiligheid van het OndernemingsDossier en bij de (private) partijen die er voor verantwoordelijk zijn.. Op dit moment zijn de koploperbranches bezig een serviceorganisatie in te richten voor beheer en doorontwikkeling. Het ligt voor de hand om de beveiligingsaspecten daar te beleggen. • Voer eHerkenningsauthenticatie van niveau 2 aangevuld met machtiging van derden en aanvullende gegevens van een persoon (zogenoemde attributen) in, zodra dit in eHerkenning beschikbaar is. Planning is voorjaar van 2012. • Vervang certificaten die gebruik maken van verouderde encryptie (SHA-1, Secure Hash Algoritme 1) door certificaten die gebruik maken van actuele encryptie (SHA-2, Secure Hash Algoritme 2).

4.4 Standaard Bedrijfsrapportage (SBR) en eFactureren

4.4.1 Korte beschrijving

De diensten **Standaard Bedrijfsrapportage (SBR)** en **eFactureren** zijn in deze rapportage gecombineerd**.** Dit omdat beide diensten voor hun belangrijkste functionaliteit, het uitwisselen van gegevens, afhankelijk zijn van Digipoort-PI (Digipoort Proces Infrastructuur). De veiligheid van SBR en eFactureren wordt daardoor vooral bepaald door de veiligheid van Digipoort-PI.



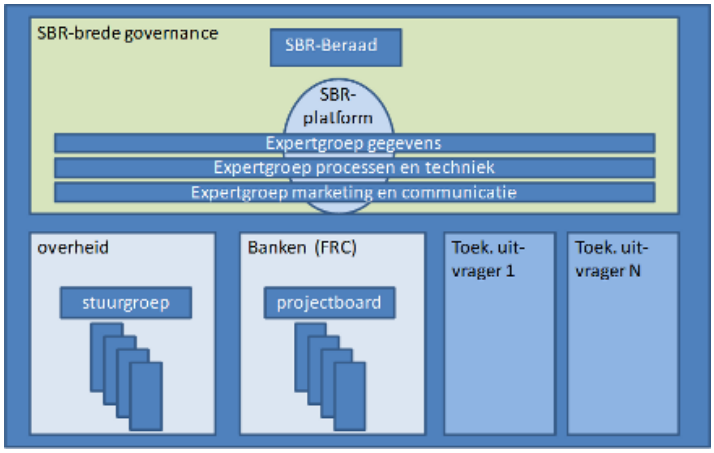
Figuur 2: Schematische weergave van Digipoort-PI tussen bedrijven en overheden.

Digipoort-PI is een beveiligde digitale poort voor communicatie tussen overheden en bedrijven, waar naast SBR en eFactureren ook andere diensten gebruik van maken (zie figuur 2). Digipoort-PI wordt beheerd door Logius en valt daarmee onder de verantwoordelijkheid van het Ministerie van BZK.

SBR en eFactureren vallen binnen de programma's van de Digitale Agenda.nl van het Ministerie van EL&I. SBR en eFactureren maken in de uitvoering gebruik van Digipoort-PI, waar Logius, en daarmee het Ministerie van BZK verantwoordelijk voor is. Het onderzoek richt zich op de diensten uit de Digitale Agenda.nl, maar in overleg met de opdrachtgever en met instemming van de directeur van Logius is ook Digipoort-PI in het onderzoek meegenomen, aangezien dit een essentieel onderdeel van de dienst uitmaakt.

Standaard Bedrijfsrapportage (SBR)
De dienst Standaard Bedrijfsrapportage (SBR) zorgt ervoor dat ondernemers minder werk hebben aan het maken en aanleveren van verplichte rapportages aan overheden en banken. Het eenmaal inrichten van de bedrijfsrapportages volgens SBR zorgt voor een efficiënt (her)gebruik van gegevens. Zo hoeven de verschillende rapportages niet handmatig samengesteld en verzonden te worden.

Vanaf 2013 zal SBR de enige aanlevermethode zijn voor de aangiften inkomstenbelasting en vennootschapsbelasting van bedrijven over het belastingjaar 2012, wanneer het gaat om system-to-system aanlevering. Bedrijven kunnen voor deze aangiften dan geen gebruik meer maken van het BAPI-kanaal van de Belastingdienst. Vanaf 2014 zal dit ook gelden voor de aangiften omzetbelasting en vanaf 2015 voor de overige belastingaangiften van bedrijven.



Figuur 3: Schematische weergave van de organisatorische structuur van het Programma SBR.

Ook voor een aantal statistiekopgaven en het deponeren van de jaarrekeningen zal op termijn gelden dat SBR het enige system-to-system kanaal zal zijn.

De dienst SBR bestaat uit een afsprakenstelsel voor het opstellen van bedrijfsrapportages en een faciliteit (Digipoort-PI) voor het versturen ervan. De bedrijven en overheden die werken met SBR moeten aansluiten op Digipoort-PI en hun software dient hierop ingericht te zijn.

De verantwoordelijkheid voor de dienst SBR ligt bij Logius, in samenspel met de beleidsopdrachtgever en de uitvragende partijen. De organisatorische structuur van dit programma is schematisch weergegeven in figuur 3. Het SBR Beraad is het besluitvormende orgaan van het Programma SBR. De voorzitter is de Secretaris-generaal van het Ministerie van EL&I. Daarnaast zijn verschillende overheden en marktpartijen vertegenwoordigd.

De verantwoordelijkheid voor de faciliteit Digipoort-PI ligt bij Logius. De regievoering vanuit het Programma SBR op Logius, de eigenaar van Digipoort-PI[5], is ondergebracht bij het Ministerie van EL&I, Directie Regeldruk en ICT-beleid. Op 29 januari 2010 is het Plan Invoering SBR formeel vastgesteld met als ingangsdatum 1 januari 2010. Op basis hiervan zijn in opdrachtbrieven (2010, 2011) nadere afspraken vastgelegd tussen het Ministerie van EL&I in de rol van opdrachtgever namens het SBR Beraad en Logius als opdrachtnemer.

Het programma SBR is een tijdelijke organisatie. De planning is erop gericht om eind 2011 de overdracht van het Programma SBR aan de lijnorganisatie Logius af te ronden. Daarmee wordt het Programma SBR als zodanig afgesloten.

Status	SBR is in productie.
Eigenaar	De eigenaar van SBR is niet expliciet bepaald. Feitelijk is het gemeenschappelijk eigendom van alle uitvragende partijen, en Logius. Die hebben in gezamenlijkheid de doorslaggevende stem als het gaat om belangrijke beslissingen. Formeel is het Ministerie van EL&I de opdrachtgever voor het SBR programma. Daarnaast sluiten de uitvragende partijen individueel contracten af voor de diensten die zij van Logius afnemen.
Functioneel beheer	Functioneel beheer is belegd bij Logius, dat het heeft ondergebracht bij het Programma SBR. Functioneel beheer van de website van Logius, ligt bij Logius.
Applicatie beheer	Zie onder Digipoort-PI. Voor de website ligt het applicatiebeheer bij Logius, die dat bij Intermax heeft ondergebracht.
Technisch beheer	Zie onder Digipoort-PI. Voor de website ligt het technisch beheer bij Logius, die dat bij Intermax heeft ondergebracht.

eFactureren
Ieder jaar versturen bedrijven zo'n 15 miljoen facturen per post naar de overheid. Vervolgens worden deze facturen handmatig verwerkt. Dit kost veel tijd en geld. Daarom stimuleert de overheid bedrijven elektronische facturen te verzenden naar de overheid.

[5] Vanuit verschillende bronnen wordt anders tegen het “eigenaarschap” van Digipoort-PI aangekeken.

Vanaf 1 januari 2011 zijn alle ministeries aangesloten op Digipoort-PI en kunnen zij elektronische facturen ontvangen en verwerken. Bedrijven kunnen al hun facturen voor de Rijksoverheid elektronisch indienen via Digipoort-PI. Digipoort-PI controleert of de e-factuur betrouwbaar, leesbaar en verwerkbaar is en zorgt dat de e-factuur snel bij de juiste overheidsorganisatie terechtkomt.

De dienst eFactureren bestaat uit een afsprakenstelsel voor het opstellen van e-facturen en een faciliteit (Digipoort-PI) voor het versturen ervan. De bedrijven en overheden die werken met e-facturen moeten aansluiten op Digipoort-PI en hierop toegespitste software aanschaffen, of hun bestaande software hiervoor aan laten passen.

De verantwoordelijkheid voor de dienst eFactureren ligt bij het Ministerie van EL&I. Logius is als opdrachtnemer verantwoordelijk voor de operationele uitvoering en de daarvoor benodigde infrastructuur, Digipoort-PI.

De beleidsopdrachtgever (EL&I) voor de dienst eFactureren wil per 1-1-2012 de beleidsopdracht overdragen aan het Ministerie van BZK, die voor de dienst Elektronisch Bestellen en Factureren aan het Rijk beleidsopdrachtgever is. Logius blijft verantwoordelijk is voor de onderliggende infrastructuur, Digipoort-PI.

Status	eFactureren is in productie.
Eigenaar	De eigenaar van eFactureren is niet expliciet bepaald. Feitelijk is het gemeenschappelijk eigendom van alle uitvragende partijen, en Logius. Die hebben in gezamenlijkheid de doorslaggevende stem als het gaat om belangrijke beslissingen. Het Ministerie van EL&I – Directie regeldruk en ICT-beleid is beleidsopdrachtgever voor het stimuleren van eFactureren via Digipoort-PI. De Klantenraad houdt toezicht op eFactureren. De Klantenraad bestaat op dit moment uit Ministerie van Financiën, Ministerie Infrastructuur en Milieu, UWV, Gemeente Ede, Logius (directeur is voorzitter), EL&I, Logius doet secretariaa.
Functioneel beheer	Functioneel beheer is belegd bij Logius. Functioneel beheer voor de website, onderdeel van de website van Logius, ligt bij Logius.
Applicatie beheer	Zie onder Digipoort-PI. Voor de website ligt het applicatiebeheer bij Logius, die dat bij EBPI heeft ondergebracht.
Technisch beheer	Zie onder Digipoort-PI. Voor de website ligt het applicatiebeheer bij Logius, die dat bij Intermax heeft ondergebracht.

Digipoort-PI

Digipoort Proces Infrastructuur (Digipoort-PI) is een generieke voorziening voor het geautomatiseerd afwikkelen van informatie-uitwisselingsprocessen tussen bedrijven en overheden. Digipoort-PI maakt onderdeel uit van de infrastructuur van de e-overheid.

Ieder bedrijf dat is aangesloten op Digipoort-PI kan digitaal informatie uitwisselen met de overheid. Digipoort zorgt dat de informatie van een bedrijf bij de betreffende overheidsinstanties terechtkomt en

dat informatie die een overheidsorganisatie verstuurt, wordt afgeleverd bij het juiste bedrijf. Digipoort-PI zorgt onder meer voor het feitelijk versturen van standaard bedrijfsrapportages en e-facturen.

In 2009 verstuurde Digipoort-PI ongeveer 10.500 elektronische berichten. In 2010 154.000 en in 2011 waarschijnlijk ongeveer 250.000. In 2010 lopen zowel eFactureren als SBR operationeel via Digipoort-PI. Daarnaast bedient Digipoort-PI ook transacties voor het UVW.

De Werkgroep Processen is specifiek opgericht om voor partijen die op Digipoort-PI aangesloten worden de ketenprocessen te beschrijvingen en te verbeteren. In deze werkgroep zitten onder andere vertegenwoordigers van het Programma SBR, procesarchitecten, Kamer van Koophandel en Belastingdienst. De werkgroep wordt bijgestaan door een Werkgroep Compliance, bestaande uit juristen, die verifieert of aan wet- en regelgeving wordt voldaan.

De verantwoordelijkheid voor Digipoort-PI ligt bij Logius, een baten-lastendienst van het Ministerie van BZK. Een deel van het beheer van Digipoort-PI wordt uitgevoerd door marktpartijen.

Status	Digipoort is in productie.
Eigenaar	Digipoort-PI heeft geen expliciete eigenaar[6]. Operationeel verantwoordelijke voor Digipoort-PI is Logius, een baten-lastendienst van het Ministerie van BZK, gerepresenteerd door de algemeen directeur van Logius Toezichthouder is het Ministerie van BZK, gerepresenteerd door de Directeur-generaal DGOBR.
Functioneel beheer	Het functioneel beheer wordt uitgevoerd door Logius, in samenwerking met de afnemers van de Digipoort-PI dienstverlening.
Applicatie beheer	Dit wordt uitgevoerd door EBPI.
Technisch beheer	Dit wordt uitgevoerd door Equinix / EBPI.

4.4.2 Risicoprofiel

De diensten SBR en eFactureren richten zich geheel op het veilig en betrouwbaar versturen van gegevens tussen bedrijven en overheden. Vanwege het hiervoor noodzakelijke vertrouwen, moet de veiligheid van de dienst zelf onberispelijk zijn. Dit vergt een zeer hoog beveiligingsniveau voor de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de diensten SBR en eFactureren, alsmede de onderliggende infrastructuur Digipoort-PI ernstig worden beschadigd.
De maximaal toegestane uitvalsduur (MTU) is niet voor de te leveren dienstverlening vastgelegd. Voor Digipoort-PI is een serviceniveau overeenkomst Digipoort-PI opgesteld [SNO Digipoort-PI], waarbij er afspraken gemaakt zijn over het melden, beoordelen en afhandelen van incidenten. Voor incidenten met een hoge impact en urgentie staat een oplostijd van 4 uur, voor incidenten met een hoge impact of hoge urgentie staat een oplostijd van 8 uur.

[6] Vanuit verschillende bronnen wordt anders tegen het “eigenaarschap” van Digipoort-PI aangekeken.

De openstellingswindow[7] van Digipoort-PI is op 99,7% voor 24 uur per dag, 7 dagen per week, alle dagen van het jaar gesteld. De helpdesk is altijd voor calamiteiten bereikbaar.

Binnen Digipoort-PI worden persoonsgegevens verwerkt volgens klasse 2 van Wbp (wet bescherming persoonsgegevens).

Naast de directe gevolgen door incidenten met betrekking tot SBR, eFactureren en Digipoort-PI, bestaat voor de deelnemende partijen en met name voor de aanjagende partij, het Ministerie van EL&I, de reële mogelijkheid van imagoschade.

Veiligheidsaspect	Vereist beveiligingsniveau
Beschikbaarheid	Zeer hoog
Integriteit	Zeer hoog
Vertrouwelijkheid	Zeer hoog
MTU	Is niet algemeen vastgelegd. Wel zijn er afspraken gemaakt over incidentafhandeling voor Digipoort-PI (melden, beoordelen en afhandelen van incidenten, inclusief maximale oplostijden van incidenten)

4.4.3 Bevindingen

SBR

Algemeen

De dienst SBR is in een transitiefase. De taken van het Programma SBR worden op korte termijn overgebracht naar de lijnorganisatie (Logius). Volgens de huidige planning is dat eind 2011, maar inmiddels is besloten het programma nog voort te zetten in 2012.

Beleid, standaarden, processen en procedures

De huidige tijdelijke organisatie moet overgaan naar de lijnorganisatie van Logius. Omdat de overdracht uitgesteld is, zal de huidige tijdelijke organisatie en invulling van besturing-, beheer en beveiligingsprocessen nog even blijven bestaan.

Voor het afsprakenstelstel SBR is het eigenaarschap niet goed uitgekristalliseerd; dit kan tot onduidelijkheid in verantwoordelijkheden tussen de stakeholders leiden.
De taakverdeling en de werkwijze van het Programma SBR is voor een deel vastgelegd in opdrachtbrieven van het Ministerie van EL&I aan Logius. In de opdrachtbrieven is elk jaar op programma niveau een risicoanalyse en de bijbehorende mitigerende maatregelen opgenomen. Een belangrijk element hierin is het regelmatige overleg over de voortgang, issues, risico's en maatregelen.
Issues op het gebied van beveiliging worden gemeld en vanuit de opdrachtgever kan op dit gebied ook sturing worden gegeven.

Bij Kamervragen is de beleidsopdrachtgever, het Ministerie van EL&I, primair verantwoordelijk gesteld voor de dienst SBR.

[7] Met openstellingswindow wordt bedoeld de tijd dat de dienst beschikbaar is voor de gebruikers en afnemers, exclusief gepland onderhoud.

Techniek
Zie Digipoort-PI.

eFactureren

Algemeen
eFactureren is in productie bij Logius.

Beleid, standaarden, processen en procedures
Voor het afsprakenstelstel eFactureren is het eigenaarschap niet goed uitgekristalliseerd; dit kan tot onduidelijkheid in verantwoordelijkheden tussen de stakeholders leiden.
De taakverdeling en de werkwijze voor de dienst eFactureren is voor een deel vastgelegd in opdrachtbrieven van het Ministerie van EL&I aan Logius. Een belangrijk element hierin is het regelmatige overleg over de voortgang, issues, risico's en maatregelen. In de opdrachtbrieven is elk jaar op project niveau een risicoanalyse en de bijbehorende mitigerende maatregelen opgenomen. Issues op het gebied van beveiliging worden gemeld en vanuit de opdrachtgever kan op dit gebied ook sturing worden gegeven.

Bij Kamervragen is de beleidsopdrachtgever, het Ministerie van EL&I, primair verantwoordelijk gesteld voor de dienst eFactureren.

Ten aanzien van het beleidsopdrachtgeverschap zijn er verschillende beelden (deling door het Ministerie van BZK (DGOBR/FHIR) en het Ministerie van EL&I (DGB&I/RI))

Techniek
Zie Digipoort-PI.

Digipoort-PI

Algemeen
Digipoort-PI is operationeel onder verantwoordelijkheid van Logius. Logius heeft een groot deel van het applicatiebeheer en het technisch beheer uitbesteed aan externe partijen. Ongeveer 20% van het beheer van Digipoort-PI wordt uitgevoerd door Logius.

Digipoort-PI is een onderdeel van ketens tussen bedrijven en overheden. Indien Digipoort-PI niet beschikbaar is, heeft dat direct gevolgen voor de daarop gebaseerde diensten SBR en eFactureren en daarmee voor de processen bij de organisaties die deze diensten gebruiken. Voor het functioneren van de ketens is het van groot belang dat de ketenafhankelijkheden goed worden gemanaged. Deze functie is nog nauwelijks belegd.

Het restrisico van Digipoort is door de operationeel verantwoordelijke in kaart gebracht en gedeeld met de stuurgroep Digipoort-PI.

Beleid en standaarden
Er is voor de verschillende beherende partijen voor Digipoort-PI één informatiebeveiligings-aanpak. De externe partijen zijn verantwoordelijk voor de informatiebeveiliging van de door hen beheerde delen. Informatiebeveiliging bij Logius en de externe partijen is ingericht volgens de beveiligingstandaard ISO 27001. In de uitbestedingsovereenkomsten zijn aanvullende eisen met betrekking tot informatiebeveiliging gesteld, bijvoorbeeld dat de gebruikte software voldoende recent is en voorzien is van recente patches.

Processen en procedures
Logius heeft een risicoanalyse op het niveau van Digipoort-PI opgesteld. Deze analyse wordt elke twee jaar bijgesteld. Tevens is een baseline gedefinieerd om binnen Digipoort-PI ten minste te kunnen werken met gegevens van Wbp (wet bescherming persoonsgegevens) risicoklasse 2. Wbp risicoklasse 2 betekent gevoelige persoonsgegevens of een grote hoeveelheid persoonsgegevens [zie Wbp].

De benodigde maatregelen zijn opgenomen in het normenkader van Digipoort-PI. De partijen waaraan Logius heeft uitbesteed, moeten een eigen risicoanalyse uitvoeren en de in ISO 27001 voorgeschreven ISMS (Information Security Management System) uitvoeren. De implementatie van de maatregelen wordt gemonitoord.

De belangrijkste beheerprocessen zijn gebaseerd op ITIL (Information Technology Infrastructure Library, een breed geaccepteerd referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie) en zijn goed beschreven.

Voor incidentbeheer maakt Logius gebruik van het systeem Clientele ITSM (applicatie voor IT service management). Veiligheidsincidenten worden altijd met de hoogste prioriteit (prioriteit 1) behandeld. Handmatig wordt beoordeeld of een incident tot een wijziging leidt en dientengevolge in het wijzigingsproces gebracht moeten worden.

Voor wijzigingsbeheer, ook ondersteund met behulp van Clientele, is een change advisory board (CAB) ingesteld. Voor iedere wijziging die impact heeft op de functionaliteit wordt een impactanalyse gemaakt. Indien nodig wordt ook een deltarisicoanalyse uitgevoerd. De status van de wijziging wordt effectief gemonitoord.

Voor enkele beheerprocessen staan nog enkele acties open, waaronder:
- Het beschrijven van wijzigingsbeheer voor SBR Digipoort-PI processen.
- Het beschrijven van behoeftemanagement voor SBR.
- Het beschrijven van procesbeheer voor SBR Digipoort-PI processen.

Digipoort-PI wordt jaarlijks extern geaudit. Dit betreft alle uitvoerende partijen. De laatste externe audit was eind 2010. Eind 2011 is de volgende externe audit gepland. De externe audits leiden tot een TPM (Third Party Mededeling), waarin de resultaten van de onafhankelijke audit zijn verwoord. De resultaten van de audits worden gebruikt om de volgende verbetercyclus in te gaan conform ISO 27001. Logius bewaakt de kwaliteit van de audits. Daarnaast wordt de kwaliteit van de audits regelmatig beoordeeld door de Rijksauditdienst (RAD). De beveiligingsfunctionaris van Logius bewaakt het oplossen van de geconstateerde issues.

Techniek
Jaarlijks worden penetratietesten uitgevoerd. Daarvoor is een mantelovereenkomst afgesloten met verschillende leveranciers. De laatste penetratietest is uitgevoerd door Madison Gurkha. De eerstvolgende is gepland op het moment de nieuwe Digipoort-PI infrastructuur wordt opgeleverd (verwachting juli 2012).
De in de penetratietesten gevonden gebreken worden meegenomen in het wijzigingsbeheer en worden door een beveiligingsfunctionaris van Logius bewaakt op implementatie. De bevindingen van de laatste penetratietesten zijn allemaal afgehandeld.

Binnen Digipoort wordt geen gebruik gemaakt van detectiesystemen voor het detecteren van hackers. In het verleden is een analyse gemaakt door de eerdere systeemeigenaar (de Belastingdienst) waaruit bleek dat dit niet nodig was, maar deze analyse is niet meer aanwezig.

De architectuur van de Digipoort-PI laat een duidelijke scheiding tussen de primaire en de beheerprocessen zien. De beheerders hebben beveiligde remote toegang tot beheersystemen. Het netwerk waar gegevens worden opgeslagen (SAN, *Storage Area Network*) is afgeschermd.

Digipoort-PI is fysiek gescheiden van andere systemen. Er zijn gescheiden (en meerdere) omgevingen zijn voor Ontwikkeling, Test, Acceptatie en Productie (OTAP omgevingen). Tevens is er een uitwijkvoorziening. De beheersystemen voor de productieomgeving zijn gescheiden van de beheersystemen voor de andere omgevingen.

Binnen Digipoort-PI wordt gebruikt gemaakt van PKIOverheid certificaten voor alle verbindingen. Er werd gebruik gemaakt van Diginotar certificaten. Al deze certificaten zijn vervangen. Er wordt overal gebruik gemaakt van certificaten op basis van SHA-2 (Secure Hash Algoritme 2, actuele internationale standaard, behalve voor een specifieke verbinding met de Belastingdienst waar een load balancer staat die nog uitsluitend met SHA-1 (Secure Hash Algoritme 1, internationale standaard, verouderd) overweg kan. Migratie voor deze verbinding naar SHA-2 staat gepland voor 21 november 2011.

4.4.4 Oordeel

SBR

Algemeen
Voor een tijdelijk geregelde dienst is de inrichting ervan tamelijk goed op orde, maar het tijdelijke karakter is een risico voor de continuïteit van de dienst. De uitvoering van de dienst is goed belegd, maar het eigenaarschap is nog niet goed uitgekristalliseerd. Dit heeft vooral consequenties voor de functionaliteit en het imago van deze dienst en niet voor de veiligheid ervan. De componenten die invloed hebben op de veiligheid van de dienst zijn namelijk geconcentreerd in de onderliggende dienst Digipoort-PI.

Beleid, standaarden, processen en procedures
Door het uitstel van de overdracht naar de lijnorganisatie van Logius blijft de huidige tijdelijke organisatie bestaan.

De sturing met (gestandaardiseerde) opdrachtbrieven is van voldoende kwaliteit. In de opdrachtbrieven zijn geen specifieke informatiebeveiligingsrisico's benoemd.

Imagoschade voor het Ministerie van EL&I als beleidsopdrachtgever ten aanzien van het merk SBR krijgt in de opdrachtbrieven voldoende aandacht. Er zijn afspraken gemaakt over hoe te handelen bij calamiteiten en over woordvoering. Ten aanzien van de uitvoering van SBR heeft het Ministerie van EL&I als beleidsopdrachtgever slechts een beperkte rol.
Indien er zaken mis gaan in de uitvoering zijn andere partijen directer betrokken, zoals overheidsdienstverleners, Logius, bedrijven. Aangezien er in het stelsel met meerdere aangesloten partijen zijn, kan er imagoschade ontstaan bij meerdere partijen (olievlek werking).

Techniek
Zie Digipoort-PI.

eFactureren

Algemeen
De dienst eFactureren is nog in ontwikkeling. De uitvoering van de dienst is goed belegd, maar eigenaarschap is nog niet goed uitgekristalliseerd. Dit heeft vooral consequenties voor de functionaliteit en het imago van deze dienst en niet voor de veiligheid ervan. De componenten die invloed hebben op de veiligheid van de dienst zijn namelijk geconcentreerd in de onderliggende dienst Digipoort-PI.

Beleid, standaarden, processen en procedures
De sturing met (gestandaardiseerde) opdrachtbrieven is van voldoende kwaliteit. In de opdrachtbrieven zijn geen specifieke informatiebeveiligingsrisico's benoemd.

Imagoschade voor het Ministerie van EL&I als beleidsopdrachtgever ten aanzien van het merk eFactureren krijgt in de opdrachtbrieven voldoende aandacht. Er zijn afspraken gemaakt over hoe te handelen bij calamiteiten en over woordvoering. Ten aanzien van de uitvoering van eFactureren heeft het Ministerie van EL&I als beleidsopdrachtgever slechts een beperkte rol. Indien er zaken mis gaan in de uitvoering zijn andere partijen directer betrokken, zoals overheidsdienstverleners, Logius, bedrijven. Aangezien er in het stelsel met meerdere aangesloten partijen zijn, kan er imagoschade ontstaan bij meerdere partijen (olievlek werking).

Techniek
Zie Digipoort-PI.

Digipoort-PI

Algemeen
Digipoort-PI en het beheer ervan zijn professioneel ingericht.

De ketenafhankelijkheden ten aanzien van Digipoort-PI en de daarop draaiende diensten als SBR en eFactureren is nog nauwelijks terug te vinden in de inrichting en organisatie van deze verschillende diensten.

Beleid en standaarden
Voor informatiebeveiliging wordt afdoende gebruik gemaakt van de standaard ISO 27001.

Processen en procedures
Logius en de uitvoerende beheerpartijen maken risicoanalyses en houden deze bij. De beheerprocessen en incidentafhandeling zijn afdoende ingericht.

Ketenprocessen van bedrijf tot dienstaanbieders komen beheerst tot stand met betrokkenheid van ketenpartners, inclusief verificatie op compliance met regelgeving.

Er is een baseline gedefinieerd die voldoet om gegevens van Wbp klasse 2 [Wet bescherming persoonsgegevens, Wbp] te verwerken en die voor Digipoort-PI gevolgd wordt. Dit is getoetst aan wet- en regelgeving.

De documentatie is op orde. Uit de interviews en documentatie blijkt dat Logius de processtappen tot verbetering onderneemt zoals bedoeld in ISO 27001. Audits worden regelmatig uitgevoerd op de uitvoerende beheerpartijen en Logius zelf. De bevindingen worden gedeeld met stakeholders en omgezet in maatregelen en de implementatie ervan gemonitoord.

Techniek
Jaarlijks worden penetratietesten uitgevoerd. De rapportage over en de opvolging van de bevindingen is goed geregeld. Penetratietesten geven, naast audits, een beperkte toetsing op het gebied van veiligheid. Penetratietesten zijn dan ook bedoeld als aanvulling op andere beveiliging- en toetsingsmaatregelen. Aanvullende aandacht wordt aanbevolen voor het detecteren van hackers en andere proactieve technische maatregelen.

De architectuur van de Digipoort-PI is doordacht. Digipoort-PI is fysiek gescheiden van andere systemen. Er zijn verschillende omgevingen voor Ontwikkeling, Test, Acceptatie en Productie (OTAP). Tevens is er een uitwijkvoorziening.

Binnen Digipoort-PI wordt gebruikt gemaakt van PKI-Overheid certificaten voor alle verbindingen. Er wordt steeds gebruik gemaakt van certificaten op basis van SHA-2 (Secure Hash Algoritme 2, actuele internationale standaard).

4.4.5 Aanbevelingen

SBR en eFactureren

Algemeen
Geef aandacht aan het eigenaarschap van de diensten SBR en eFactureren, eventueel op delen van deze diensten.

Beleid, standaarden, processen en procedures
Voer ten behoeve van de voorgenomen stap van ingroei van de SBR-programma-"cel" binnen Logius een risicoanalyse per service over de ketenpartners uit in verband met de gewenste gegarandeerde dienstverlening (bron: bevindingen Digipoort-PI, gemis overzicht ketenprocessen).

Oefen escalatietrajecten met stakeholders aan de hand van scenarios voor SBR en eFactureren en leg dit vast in procedures. Zorg dat de verantwoordelijkheden en bevoegdheden duidelijk en vastgelegd zijn en dat hierover consensus bestaat.

Techniek
Zie Digipoort-PI.

Digipoort-PI

Algemeen
Inventariseer hoe de verantwoordelijkheden en bevoegdheden liggen met betrekking tot de betrokken partijen voor SBR, eFactureren en Digipoort-PI en zorg dat de verantwoordelijkheden

en bevoegdheden duidelijk en vastgelegd zijn en dat hierover consensus bestaat, inclusief afspraken over ketenverantwoordelijkheden.

Beleid en standaarden
Geen issues.

Processen en procedures
Geen issues.

Techniek
Onderzoek in hoeverre het detecteren van hackers noodzakelijk of wenselijk is voor Digipoort-PI en implementeer daar zo nodig systemen voor.

4.4.6 Samenvatting

Inleiding:
De diensten **Standaard Bedrijfsrapportage (SBR)** en **eFactureren** zijn in deze rapportage gecombineerd, omdat beide diensten voor hun belangrijkste functionaliteit, het uitwisselen van gegevens, afhankelijk zijn van dezelfde onderliggende infrastructuur, Digipoort-PI (Digipoort Proces Infrastructuur). Ook **Digipoort-PI** is in het onderzoek meegenomen.

De dienst **Standaard Bedrijfsrapportage (SBR)** bestaat uit een afsprakenstelsel voor het opstellen van bedrijfsrapportages en een faciliteit (Digipoort-PI) voor het versturen ervan.
De dienst **eFactureren** bestaat uit een afsprakenstelsel voor het opstellen van e-facturen en een faciliteit (Digipoort-PI) voor het versturen ervan.

Digipoort Proces Infrastructuur (Digipoort-PI) is een generieke voorziening voor het geautomatiseerd afwikkelen van informatie-uitwisselingsprocessen tussen bedrijven en overheden. Digipoort-PI maakt onderdeel uit van de infrastructuur van de e-overheid. Digipoort-PI zorgt voor het feitelijk uitwisselen van standaard bedrijfsrapportages en e-facturen. De operationele dienstverlening van Digipoort-PI komt tot stand onder de verantwoordelijkheid van Logius, een onderdeel van het Ministerie van BZK.

Risicoprofiel van de diensten:
De diensten SBR en eFactureren richten zich geheel op het veilig en betrouwbaar versturen van gegevens tussen bedrijven en overheden. Vanwege het hiervoor noodzakelijke vertrouwen, moet de veiligheid van de dienst zelf onberispelijk zijn. Dit vergt een zeer hoog beveiligingsniveau voor de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de diensten SBR en eFactureren, alsmede de onderliggende infrastructuur Digipoort-PI ernstig worden beschadigd.

De maximaal toegestane uitvalsduur is niet specifiek vastgelegd. Wel zijn er afspraken gemaakt over incidentafhandeling voor Digipoort-PI (melden, beoordelen en afhandelen van incidenten, inclusief maximale oplostijden).

Binnen Digipoort-PI worden persoonsgegevens verwerkt van risicoklasse 2[8] van Wbp (wet bescherming persoonsgegevens). Digipoort-PI heeft daarvoor de vereiste beveiligingsmaatregelen getroffen.

Naast de directe gevolgen door incidenten met betrekking tot SBR, eFactureren en Digipoort-PI, bestaan voor de deelnemende partijen - en met name voor de aanjagende partij, het Ministerie van EL&I - de reële mogelijkheid van imagoschade.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse(s) aanwezig?

Voor eFactureren en SBR zijn jaarlijks risicoanalyses op strategisch-tactisch niveau opgesteld. Voor Digipoort-PI zijn risicoanalyses gemaakt en deze worden goed bijgehouden, conform ISO 27001. Implementatie van de maatregelen wordt gemonitoord.

Veiligheid in het ontwerp geborgd?

Voor de afsprakenstelstels SBR en eFactureren is het eigenaarschap niet goed uitgekristalliseerd, maar de veiligheid is niet direct in het geding.

In het ontwerp speelt voor SBR en eFactureren veiligheid vooral een rol binnen Digipoort-PI. In het ontwerp van Digipoort-PI is veiligheid een belangrijk criterium geweest. Bij het ontwerp van de beheer- en beveiligingsprocessen is gebruik gemaakt van de beveiligingstandaard ISO 27001.

Veiligheid in de beheerfase geborgd?

De beheer- en beveiligingsprocessen op niveau Digipoort-PI zijn goed ingericht. Het huidige beveiligingsniveau is in overeenstemming met de gespecificeerde behoefte. De implementatie van nieuwe maatregelen naar aanleiding van wijzigingen uit de risicoanalyse wordt gemonitoord.

Risico's voldoende afgedekt?

De risico's voor SBR en eFactureren, voor zover deze betrekking hebben veiligheid, vallen vallen op geboden functionaliteit van de diensten na binnen Digipoort-PI. De risico's voor Digipoort-PI lijken op basis van de verkregen informatie voldoende afgedekt te zijn.

Om imagoschade te beperken zijn er tussen Logius en Ministerie van EL&I afspraken gemaakt over woordvoering in geval van incidenten. Aangezien SBR en eFactureren stelsels zijn met meerdere aangesloten partijen kan er imagoschade ontstaan bij meerdere partijen (olievlek werking).

Is de feitelijke werking van de elektronische dienst veilig?

Worden de veiligheidsmaatregelen uitgevoerd zowel in de front- als de backoffice?

Alle uitvoering van beveiligingsmaatregelen zit in Digipoort-PI en bij de organisaties die op Digipoort-PI aangesloten zijn. De beveiliging van Digipoort-PI is goed aangepakt, hetgeen het vertrouwen geeft dat Digipoort-PI voldoende veilig is.

Wie controleert dit?

Logius en de onderliggende uitvoerders worden jaarlijks geaudit. Daarnaast worden regelmatig penetratietesten uitgevoerd.

Risico's voldoende afgedekt?

[8] Risicoklasse 2 betreft gevoelige persoonsgegevens, of grote hoeveelheden persoonsgegevens.

Het gekozen beveiligingsniveau is goed en de daarvoor benodigde maatregelen zijn geïmplementeerd. Dit betekent overigens niet dat er geen beveiligingsincident kan optreden, maar dat een goed beveiligingsniveau gekozen en geïmplementeerd is.
Oordeel: Voor Digipoort-PI zijn veiligheid en beheer goed geregeld. SBR en eFactureren zijn afsprakenstelsels. Voor SBR en eFactureren is het eigenaarschap niet goed uitgekristalliseerd, maar de veiligheid is niet direct in het geding. De risico's voor SBR en eFactureren, voor zover deze betrekking hebben veiligheid, vallen binnen Digipoort-PI.
Aanbevelingen: **SBR en eFactureren:** • Geef aandacht aan het eigenaarschap van de diensten SBR en eFactureren, eventueel op delen van deze diensten. • Voer ten behoeve van de voorgenomen stap van ingroei van de SBR-programma-"cel" binnen Logius een risicoanalyse per service over de ketenpartners uit in verband met de gewenste gegarandeerde dienstverlening. • Oefen escalatietrajecten met stakeholders aan de hand van scenarios voor SBR en eFactureren en leg dit vast in procedures. Zorg dat de verantwoordelijkheden en bevoegdheden duidelijk en vastgelegd zijn en dat hierover consensus bestaat. **Digipoort-PI:** • Inventariseer de verantwoordelijkheden en bevoegdheden m.b.t. SBR, eFactureren en Digipoort-PI, maak ze duidelijk en leg ze vast. • Onderzoek in hoeverre het detecteren van hackers noodzakelijk of wenselijk is voor Digipoort-PI en implementeer daar zo nodig systemen voor.

4.5 eHerkenning

4.5.1 Korte beschrijving

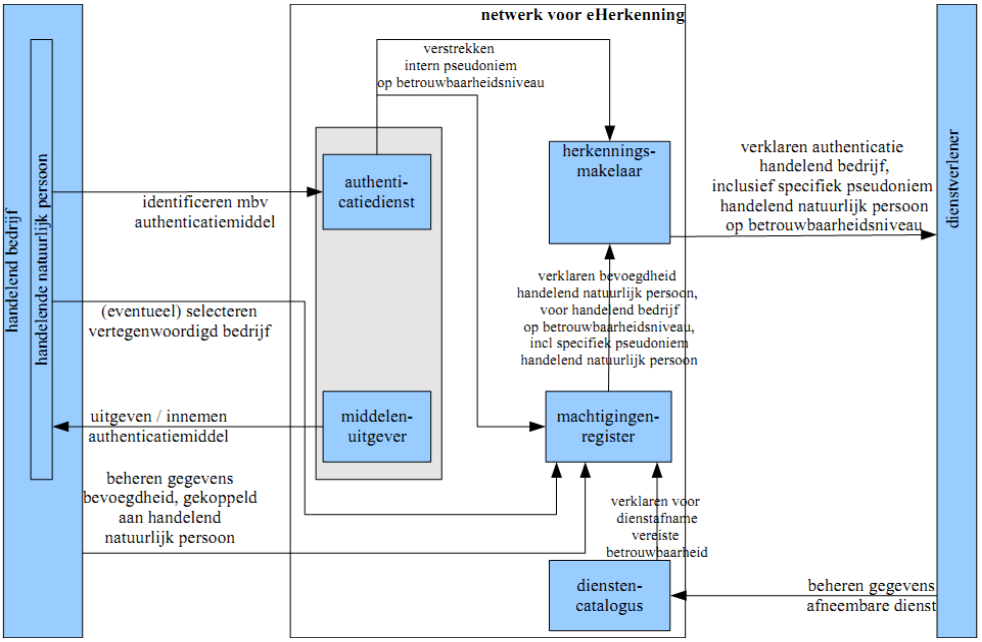
eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij (overheids)dienstverleners. Bedrijven kunnen met hun eHerkenningsmiddel bij steeds meer (overheids)dienstverleners terecht en hebben niet meer bij iedere dienstverlener een ander authenticatiemiddel nodig. De dienstverlener op zijn beurt weet door eHerkenning precies met welk bedrijf hij zaken doet en of de betreffende persoon bevoegd is om namens dat bedrijf zaken te doen met de dienstverlener. Zelf hoeft de dienstverlener daarvoor geen eigen middelen voor identificatie en authenticatie uit te geven en te beheren.

Voor Nederland is een verdere ontwikkeling van e-diensten van groot belang. eHerkenning is daarvoor cruciaal. Vandaar dat het voormalige ministerie van EZ in 2009 het initiatief heeft genomen om de evidente belangen van bedrijven en (overheids)dienstverleners bij eHerkenning te bundelen.

De kern van de oplossing is een netwerk voor eHerkenning, waarin marktpartijen – de zogenaamde deelnemers – samenwerken om herkenningsdiensten te leveren (zie onderstaande figuur 4). In dit netwerk nemen partijen deel die authenticatiemiddelen uitgeven en bijbehorende diensten verlenen. Bestaande en toekomstige authenticatiemiddelen – zoals gebruikersnaam/wachtwoorden, card readers, maar ook mobiele telefoons en eenmalige TANs – kunnen zo worden gebruikt. Ook nemen partijen deel die machtigingen van bedrijven registreren en hierover informatie verstrekken. Via het netwerk worden partijen met hun authenticatiemiddelen en machtigingen gekoppeld aan (overheids)dienstverleners die hun diensten elektronisch willen ontsluiten en bedrijven die diensten van deze dienstverleners willen afnemen. Er zijn vier verschillende rollen gedefinieerd voor het netwerk voor eHerkenning. Iedere rol is wordt tenminste door twee deelnemers uitgevoerd. Daardoor wordt de kwetsbaarheid van eHerkenning verminderd. Er is geen single point of failure. Het netwerk is ingericht om herkenningsdiensten te leveren op vier niveaus van betrouwbaarheid.[9] Het maximale betrouwbaarheidsniveau is conform PKIOverheid c.q. STORK niveau 4.

Om een dergelijk netwerk voor eHerkenning te laten functioneren en evolueren, is een set van afspraken nodig: het afsprakenstelsel eHerkenning. De afsprakenset beoogt een zo beperkt mogelijke set afspraken te bevatten, die voldoende is om samenwerking en zekerheid in het netwerk eHerkenning te garanderen en tegelijk voldoende ruimte te bieden om competitieve proposities van de deelnemers mogelijk te maken. Daartoe bevat het afsprakenstelsel allereerst bepalingen over de te leveren dienstverlening, de soorten rollen in het netwerk en de relaties tussen die rollen. Verder bevat het stelsel afspraken over de precieze werking van het netwerk: technische relaties, ondersteunde functionaliteit, kwaliteit van gegevens en dienstverlening. Ook zijn afspraken opgenomen over de onderliggende infrastructuur: welke standaarden worden gehanteerd en welke berichten en koppelvlakken worden ondersteund. Ten slotte bevat het stelsel afspraken over beheer en beveiliging en over de handhaving van de gemaakte afspraken, om de werking van het netwerk en het vertrouwen in het netwerk conform het afsprakenstelsel te waarborgen.
De ontwikkeling en het beheer van eHerkenning op stelselniveau worden in dit stadium nog uitgevoerd door een projectorganisatie en een Tijdelijke Beheerorganisatie (TBO).

[9] De niveaus van betrouwbaarheid zijn beschreven in “Afsprakenstelsel eHerkenning – Betrouwbaarheidsniveaus”.



Figuur 4:schematisch overzicht eHerkenning

Besluitvormingsprocessen over onder meer nieuwe functionaliteiten en informatiebeveiligingsissues vinden plaats binnen een zogenaamd Kernteam, Bestuur en een Wijzigingsadviesraad (WAR) waarin deelnemers aan het netwerk zijn betrokken. Ook is er een Gebruikersraad met daarin (vertegenwoordigers van) overheidsdienstverleners. De Tijdelijke Beheerorganisatie, als onderdeel van de projectorganisatie, coördineert en ondersteunt hierbij. De planning is erop gericht om per april 2012 het tactische en operationele beheer over te dragen aan Logius. Daarmee wordt het project als zodanig afgesloten.

Status	De ontwikkeling en het beheer van eHerkenning worden uitgevoerd binnen een projectorganisatie. De planning is erop gericht om per april 2012 het project eHerkenning af te ronden en over te dragen aan een staande organisatie (Logius). Daarmee bevindt het project eHerkenning zich in een transitiefase.
Eigenaar	Eigenaar is het Ministerie van EL&I, gerepresenteerd door Nicole Kroon, gedelegeerd aan Marc Hameleers en Freek van Krevel. Toezicht wordt uitgeoefend door het bestuur van eHerkenning, bestaande uit overheidsmarktpartijen en dienstaanbieders in het stelsel, ICTU en het Ministerie van EL&I, facilitair ondersteund door de TBO. Na de overdracht aan Logius wordt voor de bestuursfunctie een Stelselraad in het leven geroepen.
Functioneel beheer	Functioneel beheer op stelselniveau wordt uitgevoerd binnen de projectorganisatie door het kernteam en de WAR. Functioneel beheer voor de herkenningsdiensten wordt uitgevoerd door de deelnemers.
Applicatiebeheer	Dit wordt uitgevoerd door de deelnemers. De website wordt beheerd door de TBO. Het beheer hiervan gaat na overdracht naar Logius.
Technisch beheer	Dit wordt uitgevoerd door de deelnemers. De testtool wordt beheerd door de TBO. Het beheer hiervan gaat na overdracht naar Logius.

4.5.2 Risicoprofiel

eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij (overheids)dienstverleners. Vanwege het hiervoor noodzakelijke vertrouwen, moet de veiligheid van de dienst zelf zeer goed op orde zijn. Dit stelt stringente eisen aan de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de dienst ernstig worden beschadigd.
De eisen aan de beschikbaarheid zijn beschreven in het afsprakenstelsel (Service Level). Iedere deelnemer moet gedurende de openstellingsduur (7:00 uur – 24:00 uur) voor 99,2% (gemeten per kalendermaand) gegarandeerd en volledig beschikbaar zijn. De maximaal toegestane uitvalsduur (MTU) voor iedere deelnemer is vier uur binnen de openstellingsduur. Op stelselniveau kan de maximale uitvalsduur in principe hoger uitvallen omdat meerdere partijen in dezelfde keten achtereenvolgens maximaal vier uur uit zouden kunnen vallen.Sommige partijen binnen de dienst eHerkenning verwerken persoonsgegevens. Daar waar persoonsgegevens verwerkt worden, is de Wbp (wet bescherming persoonsgegevens) van toepassing.
Naast de directe gevolgen door incidenten met betrekking tot eHerkenning, bestaat voor alle deelnemende partijen en met name voor de ‘eigenaar’, het Ministerie van EL&I, de reële mogelijkheid van imagoschade.

Veiligheidsaspect	Vereist beveiligingsniveau
Beschikbaarheid	Hoog
Integriteit	Zeer hoog
Vertrouwelijkheid	Laag tot zeer hoog, afhankelijk van het gekozen authenticatieniveau
Maximaal toegestane uitvalsduur (MTU)	4 uur per deelnemer binnen openstellingsduur (7:00 uur – 24:00 uur)

4.5.3 Bevindingen

Algemeen
De dienst eHerkenning is in een transitiefase. Ontwikkeling en beheer zijn binnen een projectorganisatie belegd. Deze belegging is daardoor tijdelijk. De besturing-, beheer- en beveiligingsprocessen op stelselniveau zijn nog niet helemaal uitgewerkt en uitgekristalliseerd. Bovendien is de governance voor de volgende beheerfase van het eHerkenningstelsel nog niet goed geregeld. Het Ministerie van EL&I werkt hier momenteel aan.

Beleid en standaarden
Besturing van en toezicht op het eHerkenningstelsel zijn nog onvoldoende vastgelegd in het afsprakenstelsel.

Als incidenten met betrekking tot eHerkenning optreden, bestaat voor de deelnemende partijen en met name voor de ‘eigenaar’, het Ministerie van EL&I, de reële mogelijkheid van imagoschade.

Processen en procedures
Voor het eHerkenningstelsel is een risicoanalyse op stelselniveau uitgevoerd. Daarnaast heeft TBO voor de eigen beheer- en beveiligingsprocessen een risicoanalyse uitgevoerd. Beide risicoanalyses zijn niet

door een onafhankelijke partij gereviewd. Bovendien ontbreken de gap-analyses voor het monitoren van de implementatiestatus van de te treffen maatregelen.

De beheer- en beveiligingsprocessen op stelselniveau op stelselniveau zijn nog niet allemaal (goed) ingericht. Incident- en wijzigingsbeheer op stelselniveau zijn onderdeel van het afsprakenstelsel en conform deze afspraken ingericht. Het incidentbeheer wordt ondersteund door de tool Mantis. Het kleine aantal geregistreerde incidenten doet vermoeden dat de deelnemers nog niet alle relevante incidenten melden. Voor wijzigingsbeheer is een wijzigingsadviesraad (WAR) ingesteld. De administratie over wijzigingen en daaruit volgende releases wordt handmatig bijgehouden. Voor elke wijziging wordt, indien nodig, een deltarisicoanalyse gedaan. Er is geen monitoring van de implementatiestatus van de wijzigingen.
De communicatieprocessen en -procedures voor calamiteiten of grootschalige incidenten zijn nog onvoldoende beschreven.

De beheer- en beveiligingsprocessen op deelnemerniveau zijn bij de deelnemers belegd en moeten daar zodanig zijn ingericht dat tegemoet gekomen kan worden aan de afspraken in het afsprakenstelsel. Onderdeel hiervan is dat de deelnemers gecertificeerd moeten zijn voor de beveiligingsstandaard ISO 27001:2005 en het gemeenschappelijk normenkader beveiliging eHerkenning.

De conformiteit van de betrokken partijen worden in principe getoetst met behulp van audit, penetratietesten en ketentesten. Momenteel is er nog geen stelselaudit geweest. Nieuwe deelnemers krijgen geen toetredingsaudit in opdracht van het Ministerie van EL&I, maar mogen zelf conformiteit met ISO 27001:2005 en het gemeenschappelijk normenkader beveiliging eHerkenning laten auditen.

Techniek
Het afsprakenstelsel specificeert organisatorische, procedurele en technische maatregelen en volgt daarbij voor de informatiebeveiliging de standaard ISO 27001:2005. Het afsprakenstelsel laat het specificeren van een groot deel van de technische maatregelen over aan iedere deelnemer zelf. Dit betekent dat uiteindelijk wordt vertrouwd op de audits die plaatsvinden. Deze audits geven echter geen uitsluitsel over de selectie van technische maatregelen, aangezien de inhoudelijke toetsing van de risicoanalyse en de gap-analyse hiervan geen verplicht onderdeel uitmaakt. Als gevolg is het onduidelijk welke deelnemer welke technische maatregelen getroffen heeft. Zo wordt bijvoorbeeld in het afsprakenstelsel geen gebruik voorgeschreven van systemen voor het detecteren van hackers en andere proactieve technische maatregelen, zodat iedere deelnemer daarover een eigen afweging maakt.

Penetratietesten worden halfjaarlijks uitgevoerd door een professionele partij. De testen worden stelselbreed uitgevoerd, dat wil zeggen op de eHerkenningsystemen van alle deelnemers. De laatste penetratietest is uitgevoerd in juni 2011 door Sogeti. De projectorganisatie overweegt een penetratietesttool aan te schaffen om tussendoor extra penetratietesten uit te voeren, bijvoorbeeld direct na implementatie van een nieuwe release.

Alle deelnemers zijn opgenomen in een zogenaamde whitelist waarmee iedere deelnemer kan controleren of een andere partij een reguliere deelnemer is. Het bestand waarin de whitelist is opgenomen wordt door TBO digitaal getekend en via twee kanalen (e-mail, WWW) gedistribueerd naar de deelnemers. Iedere update van de whitelist wordt behandeld in het reguliere wijzigingsbeheer. In het afsprakenstelsel zijn de termijnen gedefinieerd waarbinnen iedere deelnemer de whitelist vervangen moet hebben en hoe deze wordt toegepast. Iedere deelnemer meldt de geïmplementeerde

nieuwe whitelist bij TBO af. Alle certificaten die in de laatste versie van de whitelist opgenomen zijn, zijn door de onderzoekers gecontroleerd op geldigheid, scope en gebruik van SHA-2 (Secure Hash Algoritme 2, actuele internationale standaard). Bij twee certificaten werd een ongeldige uitgever geconstateerd, maar dit was onderkend door de TBO.

4.5.4 Oordeel

Algemeen
De governance voor de volgende fase van beheer van het eHerkenningstelsel is nog niet goed geregeld. EL&I is hier mee bezig. Daardoor is het onduidelijk of de continuïteit van de dienst op langere termijn geborgd kan worden.

De besturing-, beheer- en beveiligingsprocessen binnen het eHerkenningstelsel zijn op stelselniveau weliswaar nog niet helemaal uitgewerkt en uitgekristalliseerd, maar voor een tijdelijke projectorganisatie tamelijk goed op orde. Bovendien worden de besturing-, beheer- en beveiligingsprocessen van de deelnemers door middel van regelmatige audits getoetst. Het is de vraag in hoeverre het nuttig is om kort voor de overdracht aan een staande organisatie significant te investeren in het verbeteren van de besturing-, beheer- en beveiligingsprocessen op stelselniveau als bij de overdracht ten minste een deel hiervan weer moet worden herzien.

Beleid en standaarden
Besturing en toezicht ten aanzien van het eHerkenningstelsel zijn voldoende voor een tijdelijke projectorganisatie. Na het beëindigen van de transitiefase worden hogere eisen gesteld aan besturing en toezicht. Aangezien het eind van de transitiefase al in beeld is, worden voorbereidingen getroffen om besturing en toezicht voor de nieuwe situatie in te vullen.

Het is niet duidelijk welke maatregelen de beleidsopdrachtgever van eHerkenning, het Ministerie van EL&I, heeft getroffen om imagoschade te voorkomen als incidenten met betrekking tot eHerkenning optreden.

Processen en procedures
Doordat de risicoanalyses van het eHerkenningstelsel en TBO nog onvoldoende gereviewd zijn en geen gebruik wordt gemaakt van gap-analyses, zijn er in de opzet mogelijk maatregelen over het hoofd gezien en bij de implementatie maatregelen nog niet gerealiseerd.

De inrichting van de beheer- en beveiligingsprocessen op stelselniveau is voldoende voor een tijdelijke projectorganisatie. Na de overdracht worden hogere eisen gesteld aan de beheer- en beveiligingsprocessen en het regelmatig en stringent auditen hiervan. Het inhoudelijk toetsen van de risicoanalyses, het calamiteitenplan en de gap-analyses moet hiervan deel uitmaken.

De inrichting van de beheer- en beveiligingsprocessen op deelnemerniveau is belegd bij de deelnemers en hoort daar ook thuis. Noodzakelijk is dat de conformiteit van de deelnemers regelmatig en stringent getoetst wordt met behulp van audit, penetratietesten en ketentesten. Het is noodzakelijk dat regelmatig een stelselaudit bij alle deelnemers wordt uitgevoerd. Opdrachtgever voor deze audit moet het Ministerie van EL&I worden en de stelselaudit dient te worden uitgevoerd door een onafhankelijke partij. De stelselaudit zou een echte audit moeten zijn en niet alleen een review van bestaande auditrapporten. Bovendien moet de stelselaudit een inhoudelijke toetsing omvatten van de risicoanalyses en de gap-analyses. Daarnaast dient iedere nieuwe deelnemer een onafhankelijk

toetredingsaudit te doorlopen. Ook hiervoor geldt dat dit meer zou moeten zijn dan een review van een bestaand auditrapport en bovendien moet het een inhoudelijke toets van de risicoanalyse en de gap-analyse omvatten.

Techniek
De selectie van technische maatregelen wordt voor iedere deelnemer grotendeels overgelaten aan de deelnemer zelf. Hierdoor ontbreekt het aan inzicht over de voor eHerkenning getroffen technische maatregelen en ontbreken bij de deelnemers mogelijk stelselbrede beveiligingsmaatregelen, zoals systemen voor het detecteren van hackers.

Penetratietesten geven een beperkte toetsing op het gebied van veiligheid. Penetratietesten zijn dan ook bedoeld als aanvulling op andere beveiliging- en toetsingsmaatregelen. Binnen het netwerk voor eHerkenning spelen penetratietesten echter een hoofdrol voor de beveiliging. Aanvullende aandacht is nodig voor auditing en stelselbrede beveiligingsmaatregelen, zoals systemen voor het detecteren van hackers.

Het zelf aanschaffen van een penetratietesttool heeft het voordeel dat relatief snel duidelijk wordt of bij het implementeren van een nieuwe release kwetsbaarheden geïntroduceerd zijn, maar heeft als nadeel dat slechts oppervlakkige penetratietesten uitgevoerd kunnen worden, waardoor de schijnzekerheid die met diepgaande penetratietesten gecreëerd nog verder vergroot wordt.

De whitelist waarmee de deelnemers kunnen nagaan welke andere partijen deel uitmaken van het netwerk van eHerkenning functioneert naar behoren, hoewel het wijzigingsbeheer voor (certificaten in) de whitelist nog extra aandacht behoeft. De technische maatregelen die getroffen zijn om de whitelist tijdens aanmaak en distributie te beschermen zijn voldoende. Het beveiligingsniveau van de certificaten is voldoende. De onderzoekers vinden het gebruiken van correcte certificaten die buiten het eHerkenningstelsel verlopen zijn geen veiligheidsrisico, mits deze certificaten binnen een redelijke termijn (bijvoorbeeld drie maanden) vervangen zijn.

4.5.5 Aanbevelingen

Algemeen
Het Ministerie van EL&I moet de governance voor de structurele beheerorganisatie inrichten.

Stem alle nog aan te brengen proces- en procedurewijzigingen af met Logius, aangezien Logius na de overdracht verantwoordelijk wordt voor een belangrijk deel van deze processen.

Beleid en standaarden
Zet vaart achter de voorbereidingen om besturing en toezicht voor de nieuwe situatie bij Logius in te vullen. De huidige bestuur-, beheer- en beveiligingsprocessen zijn deels tijdelijk en onvolwassen ingericht. Na de overdracht kunnen deze processen in een meer volwassen structuur komen.

Inventariseer welke maatregelen de beleidsopdrachtgever van eHerkenning, het Ministerie van EL&I, moet treffen om imagoschade te voorkomen als incidenten met betrekking tot eHerkenning optreden, en implementeer deze maatregelen.

Processen en procedures
Laat de stelselrisicoanalyse en de risicoanalyse voor TBO door een onafhankelijke partij reviewen en stel gap-analyses op. Gebruik ook gap-analyses voor het monitoren van de implementatiestatus van wijzigingen.

Stel, in overleg met Logius, een calamiteitenplan op stelselniveau op. Dit plan bevat onder meer de communicatieprocessen en -procedures voor calamiteiten of grootschalige incidenten.

Stel de afspraken met betrekking tot audit zodanig bij dat de stelselaudits volwaardige audits worden die in opdracht van het Ministerie van EL&I uitgevoerd worden. Iedere stelselaudit zou een echte audit moeten zijn en niet alleen een review van bestaande auditrapporten. Bovendien moet de stelselaudit een inhoudelijke toetsing omvatten van de risicoanalyses en de gap-analyses.
Daarnaast dient iedere nieuwe deelnemer een onafhankelijk toetredingsaudit te krijgen in opdracht van het Ministerie van EL&I. Ook hiervoor geldt dat dit meer zou moeten zijn dan een review van een bestaand auditrapport en bovendien moet het een inhoudelijke toets van de risicoanalyse en de gap-analyse omvatten.

Voer een stelselaudit uit in opdracht van het Ministerie van EL&I. De stelselaudit heeft betrekking op alle stelselpartijen. Voer bij elke nieuwe deelnemer een toetredingsaudit in opdracht van het Ministerie van EL&I uit.

Techniek
Investeer niet in een eigen penetratietesttool, maar geef voorrang aan het verplicht invoeren van aanvullende stelselbrede beveiligingsmaatregelen bij de deelnemers, zoals systemen voor het detecteren van hackers, en andere proactieve technische maatregelen. Maak dit in het normenkader expliciet.

Leg het wijzigingsbeheer voor de whitelist vast, evalueer dit en pas het zo nodig aan. Stel zeker dat de verlopen certificaten binnen een redelijke termijn (bijvoorbeeld drie maanden) vervangen zijn.

4.5.6 Samenvatting

Inleiding: eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij (overheids)dienstverleners. Bedrijven kunnen met hun eHerkenningsmiddel bij steeds meer (overheids)dienstverleners terecht en hebben niet meer bij iedere dienstverlener een ander authenticatiemiddel nodig. De dienstverlener op zijn beurt weet door eHerkenning precies met welk bedrijf hij zaken doet en of de betreffende persoon bevoegd is om namens dat bedrijf zaken te doen met de dienstverlener. Zelf hoeft de dienstverlener daarvoor geen eigen middelen voor identificatie en authenticatie uit te geven en te beheren. De realisatie van eHerkenning gebeurt met een netwerk, waarin marktpartijen – de zogenaamde deelnemers – samenwerken om herkenningsdiensten te leveren. De ontwikkeling en het beheer van eHerkenning op stelselniveau worden in dit stadium nog uitgevoerd door een projectorganisatie en een Tijdelijke Beheerorganisatie (TBO).
Risicoprofiel van de dienst: eHerkenning is een gestandaardiseerde dienst voor identificatie en authenticatie van bedrijven bij

(overheids)dienstverleners. Vanwege het hiervoor noodzakelijke vertrouwen, moet de veiligheid van de dienst zelf zeer goed op orde zijn. Dit stelt stringente eisen aan de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de dienst ernstig worden beschadigd.

De eisen aan de beschikbaarheid zijn beschreven in het afsprakenstelsel (Service Level). Iedere deelnemer moet gedurende de openstellingsduur (7:00 uur – 24:00 uur) voor 99,2% (gemeten per kalendermaand) gegarandeerd en volledig beschikbaar zijn. De maximaal toegestane uitvalsduur (MTU) voor iedere deelnemer is vier uur binnen de openstellingsduur. Op stelselniveau kan de maximale uitvalsduur in principe hoger uitvallen omdat meerdere partijen in dezelfde keten achtereenvolgens maximaal vier uur uit zouden kunnen vallen.

Sommige partijen binnen de dienst eHerkenning verwerken persoonsgegevens. Daar waar persoonsgegevens verwerkt worden, is de Wbp (wet bescherming persoonsgegevens) van toepassing.

Naast de directe gevolgen door incidenten met betrekking tot eHerkenning, bestaat voor alle deelnemende partijen en met name voor de 'eigenaar', het Ministerie van EL&I, de reële mogelijkheid van imagoschade.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse(s) aanwezig? Op stelselniveau is een risicoanalyse opgesteld. Bovendien stelt elke deelnemer, inclusief de TBO, een risicoanalyse op voor het eigen deel van het eHerkenningsnetwerk. De risicoanalyses worden bijgehouden binnen het wijzigingsbeheer, maar zijn nog niet door een onafhankelijke partij gereviewd. Daardoor zijn er in de opzet mogelijk maatregelen over het hoofd gezien.

Veiligheid in het ontwerp geborgd? Veiligheid is een belangrijk criterium geweest in de ontwerpfase. Voor de ontwerp- en transitiefase is een tijdelijke stelselbeheerorganisatie, TBO, ontworpen en gerealiseerd. Deze voldoet voor de ontwerp- en transitiefase, maar niet voor de aanstaande definitieve beheerfase bij Logius.

De dienstverlening wordt geoperationaliseerd door de deelnemers (marktpartijen). Iedere deelnemer moet gecertificeerd zijn voor de beveiligingsstandaard ISO 27001 en het gemeenschappelijk normenkader beveiliging eHerkenning en daarmee aantoonbaar de eigen informatiebeveiliging op orde hebben. Aanvullende maatregelen, te weten stelselaudits en penetratietesten op het eHerkenningsnetwerk, worden ingezet om aan te tonen dat de informatiebeveiliging ook op stelselniveau geborgd is.

Veiligheid in de beheerfase geborgd? De planning is erop gericht om per april 2012 het project eHerkenning af te ronden en over te dragen aan Logius. De huidige processen en procedures binnen TBO zijn voor de transitiefase bedoeld en niet voor deaanstaande definitieve beheerfase bij Logius. Het moet nog duidelijk gemaakt worden hoe de besturing-, beheer en beveiligingsprocessen op stelselniveau bij Logius zullen worden ingericht.

Deelnemers zullen ook in de aanstaande definitieve beheerfase gecertificeerd moeten zijn voor de beveiligingsstandaard ISO 27001 en het gemeenschappelijk normenkader beveiliging eHerkenning en daarmee aantoonbaar hun informatiebeveiliging op orde hebben. In aanvulling hierop zullen uitgebreide toetredings- en stelselaudits en penetratietesten voor het eHerkenningsnetwerk moeten worden gedaan.

Risico's voldoende afgedekt? Voor de huidige transitiefase zijn de belangrijke risico's in het ontwerp van eHerkenning afgedekt. Voor de aanstaande definitieve beheerfase moet nog duidelijk gemaakt worden hoe de besturing-, beheer en beveiligingsprocessen op stelselniveau bij Logius zullen worden ingericht. Tevens is extra aandacht nodig voor het voorbereiden van de overdracht naar Logius, het opstellen van een calamiteitenplan en het structureel inrichten van de governance voor het eHerkenningstelsel. Aanvullende zekerstelling is gewenst door het reviewen van de risicoanalyses en

het bepalen of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn, het opstellen en gebruiken van gap-analyses en het vastleggen, reviewen en zo nodig aanpassen van het whitelist-proces.

Is de feitelijke werking van de elektronische dienst veilig?

Worden de veiligheidsmaatregelen uitgevoerd zowel in de front- als de backoffice? De ontworpen (deels tijdelijke) besturing-, beheer- en beveiligingsprocessen op stelselniveau en maatregelen uit het normenkader lijken op stelselniveau goed geïmplementeerd te zijn voor de huidige transitiefase.

Op deelnemerniveau wordt de uitvoering van de processen en maatregelen geborgd door de voor certificatie benodigde regelmatige audits. Een toetredingsaudit wordt door een onafhankelijke auditor wordt nog niet uitgevoerd. Er worden regelmatig penetratietesten gedaan.

Er vindt beperkte monitoring plaats op de implementatie van wijzigingen en nieuwe maatregelen op deelnemer- en stelselniveau.

Stelselaudits zijn gepland, maar nog niet uitgevoerd. In het kader van dit onderzoek zijn aanvullende audits en penetratietesten bij de deelnemers niet nodig geacht. Er moet wel vaart gemaakt worden met het uitvoeren van regelmatige stelselaudits.

Wie controleert dit? Toezicht op eHerkenning wordt uitgeoefend door het bestuur van eHerkenning, bestaande uit overheidsmarktpartijen en dienstaanbieders in het stelsel, ICTU en het Ministerie van EL&I. Het bestuur kan voor haar controlerende taak gebruik maken van de bevindingen uit de uitgevoerde audits en penetratietesten.

Risico's voldoende afgedekt? De beperkte monitoring van de implementatie van wijzigingen en nieuwe maatregelen op deelnemer- en stelselniveau en het ontbreken van uitgebreide toetredings- en stelselaudits kan leiden tot incidenten op het gebied van veiligheid.

Voor de borging van de veiligheid op termijn is het nodig om het implementeren van wijzigingen en nieuwe maatregelen effectief te monitoren en regelmatig een uitgebreide stelselaudit uit te voeren in opdracht van de beleidsopdrachtgeve van eHerkenning.

Oordeel: Het ontwerp van de besturing-, beheer- en beveiligingsprocessen op stelselniveau is voor de transitiefase voldoende veilig. Aanvullende zekerstelling is gewenst, met name door onafhankelijke review van de risicoanalyses en het bepalen of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn. Daarnaast zou er vaart gemaakt moeten worden met de transitie naar de definitieve beheerfase bij Logius en daarbij het op een hoger plan brengen van de beveiligingseisen en monitoring daarvan.

De ontworpen (deels tijdelijke) processen en de maatregelen uit het normenkader lijken op deelnemer- en stelselniveau goed geïmplementeerd te zijn, maar er vindt onvoldoende monitoring plaats op het implementeren van wijzigingen en nieuwe maatregelen. Dit kan leiden tot incidenten op het gebied van veiligheid.

Voor de borging van de veiligheid op termijn is het nodig om het ontwerp van de processen op stelselniveau te verbeteren, het implementeren van wijzigingen en nieuwe maatregelen effectief te monitoren en regelmatig een uitgebreide stelselaudit uit te voeren in opdracht van de beleidsopdrachtgever van eHerkenning.

Aanbevelingen:

- Richt de governance voor het eHerkenningstelsel structureel in en stem af met Logius.
- Zet vaart achter de voorbereidingen voor de overdracht aan Logius.
- Inventariseer de mogelijk maatregelen om imagoschade te voorkomen als incidenten m.b.t. eHerkenning optreden.
- Review de stelselrisicoanalyses en de risicoanalyse voor TBO en bepaal of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn.
- Stel op stelselniveau gap-analyses op en gebruik deze ook.

- Stel op stelselniveau een calamiteitenplan op.
- Stel de afspraken met betrekking tot audit zodanig bij dat de toetredingsaudits uniform, met dezelfde scope en diepte uitgevoerd worden.
- Regel dat iedere stelsel- en toetredingsaudit een echte audit is en zich niet beperkt tot een review van bestaande auditrapporten. Bovendien moet de stelselaudit een inhoudelijke toetsing omvatten van de risicoanalyses en de gap-analyses.
- Voer regelmatig een stelselaudit uit. De stelselaudit moet in opdracht van de beleidsopdrachtgever, het ministerie van EL&I, uitgevoerd worden.
- Investeer niet in een eigen penetratietesttool, maar geef voorrang aan het verplicht invoeren van aanvullende stelselbrede beveiligingsmaatregelen bij de deelnemers.
- Leg het wijzigingsbeheer voor de whitelist vast, evalueer dit en pas het zo nodig aan.
- Voorkom dat verlopen certificaten te lang worden gebruikt door een redelijke termijn voor vervanging van certificaten te stellen.

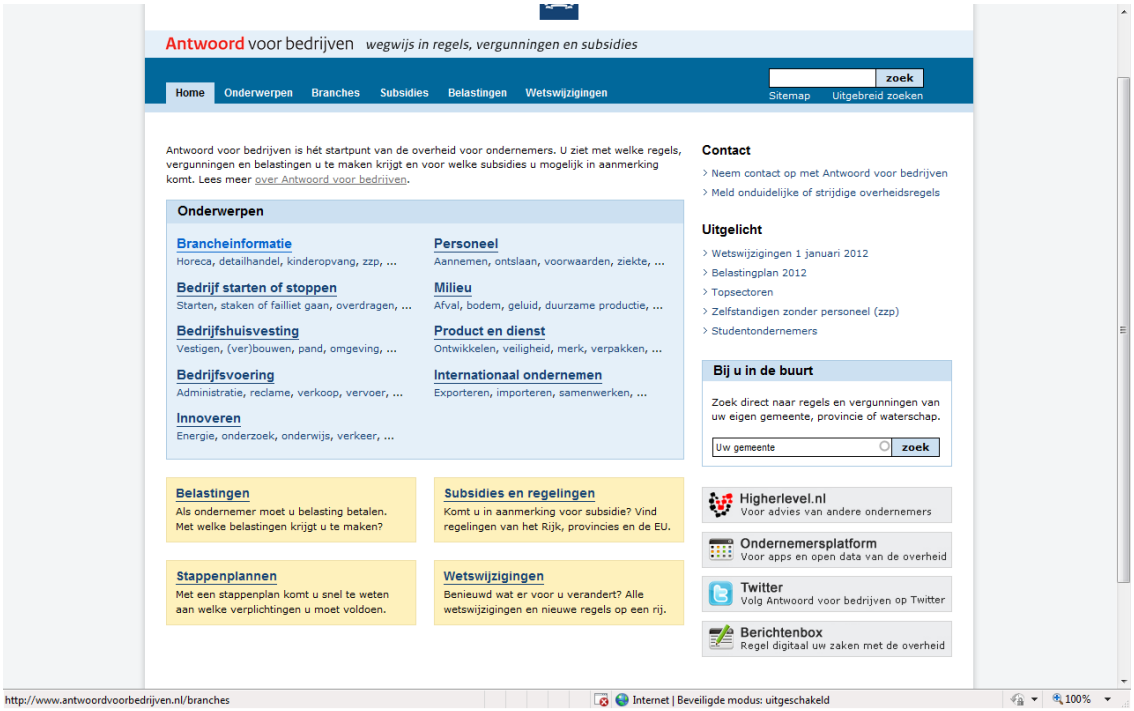
4.6 Antwoordvoorbedrijven (incl Ondernemersplatform en Open Data)

4.6.1 Korte beschrijving

Antwoordvoorbedrijven is een informatieve website die ondernemers wegwijs maakt door de grote hoeveelheid van informatie van de overheid. In de kabinetsbrief “Ondernemerspleinen”van 13 oktober 2011 van minister Verhagen is het concept van het zogenaamde digitale ondernemersplein geformuleerd. Dit concept is nog niet uitgewerkt. Antwoordvoorbedrijven is te beschouwen als een basiselement voor het realiseren van een digitaal ondernemersplein.

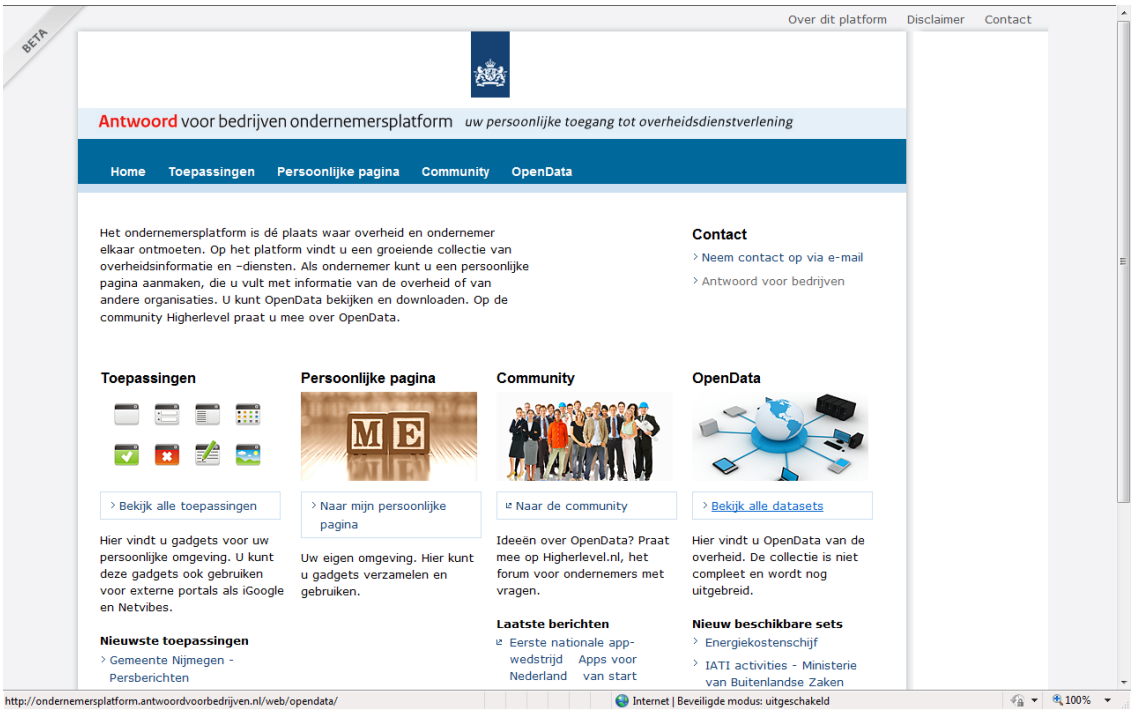
Antwoordvoorbedrijven bestaat zo’n 4 jaar in de huidige vorm en is een volwassen website. Via Antwoordvoorbedrijven kun je worden doorverwezen naar Higherlevel.nl en Twitter. Dit zijn kale links.

Antwoordvoorbedrijven is ook de toeleiding naar de berichtenbox. Deze berichtenbox is verplicht op basis van de dienstenwet.



Figuur 5: Screenshot Antwoordvoorbedrijven

Antwoordvoorbedrijven ontwikkelt op dit moment een portal (ondernemersplatform); dit platform draait op dit moment in een bèta-versie. Hierin publiceert Antwoordvoorbedrijven toepassingen, een persoonlijke pagina, community en open data.



Figuur 6: Screenshot Antwoordvoorbedrijven, ondernemersplatform

Status	AvB is een volwassen site, Ondernemersplatform is in beta-versie benaderbaar Open data en toepassingen is in het beginstadium
Eigenaar	Eigenaar is Ministerie van EL&I Toezicht wordt uitgeoefend door de Klankboardgroep voor e-Overheid voor Bedrijven
Functioneel beheer	AgentschapNL
Applicatiebeheer	Via AgentschapNL
Technisch beheer	Via AgentschapNL

4.6.2 Risicoprofiel

Antwoordvoorbedrijven verwerkt geen gevoelige of persoonlijke informatie van derden en heeft geen cruciale rol in de afhandeling van transacties van en met de overheid. Als de site enkele dagen tot een week niet beschikbaar is, is de impact laag. Hoewel er geen bijzondere eisen gesteld worden aan de gepresenteerde informatie, is het wenselijk dat de integriteit van de gegevens geborgd is.

Veiligheidsaspect	Vereist beveiligingsniveau
Beschikbaarheid	Laag
Integriteit	Medium
Vertrouwelijkheid	Laag
Maximaal toegestane uitvalsduur (MTU)	1 week

4.6.3 Bevindingen

Algemeen
De website en portal bestaat uit platte informatie en is er geen koppeling met bedrijfskritische of primaire processen. De website slaat geen persoonlijke informatie op.

Berichtenbox
Antwoord voor bedrijven is toegangspoort naar de berichtenbox, dit is een applicatie met persoonlijke gegevens waar veiligheid één van de Unique Selling Points is; de veiligheid van de Berichtenbox wordt behandeld in paragraaf 4.6.
De berichtenbox en Antwoordvoorbedrijven zijn gescheiden geïmplementeerd, als Antwoordvoorbedrijven niet benaderbaar is kan een nieuwe toegang worden gecreëerd. De Berichtenbox draait op een aparte server. Er kunnen nieuwe schermen worden ingericht. In het ontwerp van Antwoordvoorbedrijven is het een eis dat de berichtenbox benaderbaar moet zijn als Antwoordvoorbedrijven uit de lucht is.

Toepassingen
Antwoordvoorbedrijven publiceert toepassingen (“gadgets, apps”) op de portal. Op dit moment zijn het alleen nog gadgets van antwoordvoorbedrijven zelf. Zodra met toepassingen van derden gaat publiceren zal er een controle procedure moeten worden doorlopen voorafgaand aan de publicatie waarin veiligheid wordt getest. Er is een gedragscode (een *“code of conduct”*) opgesteld en er bestaat een technische scan. Bij de toepassingen worden er geen persoonlijke gegevens opgeslagen.

Persoonlijke pagina
Op de persoonlijke pagina kan de bezoeker informatie personifiëren op basis van cookies. Dit is naar analogie van iGoogle. Er wordt dus geen persoonlijke informatie opgeslagen. Gezien de aanstaande wet op cookies verwacht men dat authenticatie via de gateway AgentschapNL zal gaan plaats vinden. Implicaties hiervan zijn niet onderzocht.

Community
Niet onderzocht

Open Data
Het ondernemersplatform is een showroom waar open data collecties worden getoond. Het gebruik is minimaal en de onderzoekers verwachten geen veiligheidsissues. Er wordt hier alleen maar doorgelinkt. De collecties kunnen worden opgehaald bij de bronhouders. De bronhouders beheren de open data collecties. Op dit moment worden de links door de functioneel beheerder er handmatig ingezet. In de toekomst wordt dit geautomatiseerd. Het gebruik van de open data set is op dit moment nog minimaal.

Digitaal ondernemersplein
Er is nog geen digitaal ondernemersplein, een onderzoek naar de veiligheid van een digitaal ondernemersplein niet relevant.

Processen en Procedures

Antwoordvoorbedrijven, ondernemersplatform, open data vallen binnen het audit beleid van het functioneel beheer bij AgentschapNL.

Voor Antwoordvoorbedrijven vindt er elk jaar een penetratietest plaats. Voor de portal is er op 16 mei 2011 nog een penetratietest uitgevoerd. Aangezien de site op dit moment wordt gemigreerd zal men extra penetratietesten uitvoeren.

Via het systeem “Topdesk” worden wijzigingen doorgegeven. Beveiligingsissues krijgen altijd een hogere prioriteit.

Overdracht naar beheer voor de site wordt ingestoken door het inrichten van goede procedures en zorgen voor kennis overdracht van de bouwer naar AgentschapNL.

Beveiliging via de achterdeur is geregeld door middel van authenticatie van de redacteuren of de webmaster bij het functioneel beheer.

Bij uitval van Antwoordvoorbedrijven kan een alternatieve toegang tot de Berichtenbox worden gecreëerd. Dit is een eis voor het ontwerp van Antwoordvoorbedrijven.

Er zijn verschillende penetratietesten uitgevoerd, die de veiligheid van de platformtechniek als redelijk hebben gekwalificeerd.

Techniek

TNO heeft in maart 2011 een risico analyse uitgevoerd. Hierin wordt geconcludeerd dat het onbeschikbaar zijn van de site geen grote impact heeft. Destijds was de aanbeveling om berichtenbox benaderbaar te maken als de site niet beschikbaar is. Volgens de geïnterviewde is dit een eis en geregeld. Verder worden nog mogelijke risico’s op basis van software fouten benoemd. Dankzij een systematisch onderzoek naar computer broncode (“*Code Review*”) is dit voor nu geborgd.

Op dit moment is er een ondernemersplatform binnen Antwoordvoorbedrijven in ontwikkeling. Dit is een bèta-versie.

De techniek van Antwoordvoorbedrijven bestaat uit twee technieken. Het Content Management Systeem (CMS) voor de site. En de portaltechniek voor het ondernemersplatform. De code van de site is gereviewd en goed bevonden. Dit betekent dat de code werkt conform de gestelde eisen waaronder veiligheidseisen.

Het beheer van de site Antwoordvoorbedrijven is begin 2011 overgegaan naar AgentschapNL. Als gevolg daarvan migreert de site op dit moment naar het CMS systeem van AgentschapNL (Durpal). Dit is de standaard open source oplossing is van AgentschapNL.

De tijdelijke applicatiebeheerder van de site is Ordina, het is de doelstelling van dit applicatiebeheer wordt overgedragen naar de ICT afdeling van AgentschapNL. Als gevolg hiervan zal het functionele beheer en het applicatiebeheer bij AgentschapNL zijn belegd. Het Technische beheer wordt uitgevoerd door Prolocation.

Het ondernemersplatform wordt gebouwd in Liferay een open source portalsoftware. Tijdens de bouw van deze portal wordt de portal tijdelijk beheerd door Finalist. Het is de bedoeling dat ook dit applicatie beheer op termijn naar de ICT afdeling van AgentschapNL zal worden overgedragen. Het technische beheer is evenals de site Antwoordvoorbedrijven belegd bij Prolocation.

4.6.4 Oordeel

Algemeen
Antwoordvoorbedrijven verwerkt geen gevoelige of persoonlijke informatie van derden en heeft geen cruciale rol in de afhandeling van transacties van en met de overheid. Als de site enkele dagen tot een week niet beschikbaar is, is de impact laag. Hoewel er geen bijzondere eisen gesteld worden aan de gepresenteerde informatie, is het wenselijk dat de integriteit van de gegevens geborgd is.

De berichtenbox dient benaderbaar te zijn onafhankelijk van Antwoordvoorbedrijven. Dit is in het ontwerp meegenomen en in beheer gerealiseerd.

De techniek van site en het ondernemersplatform zijn op dit moment in ontwikkeling of in overdracht naar beheer. Dit zijn kwetsbare momenten. Dit staat op het netvlies van de toekomstige beheerder en krijgt extra aandacht. Ook extra penetratietesten kunnen worden ingepland.

Het ondernemersplatform publiceert open data en toepassingen. Deze zijn nog in het begin stadium. Procedures en codes of conduct zijn ontworpen. Dit is een goed teken.

Als de site niet werkt kan dit imagoschade opleveren. Grote impact zal dit niet hebben.

4.6.5 Aanbevelingen

Houdt veiligheid goed op de agenda van Antwoordvoorbedrijven.

Het ondernemersplatform is een portal omgeving binnen Antwoordvoorbedrijven dit in ontwikkeling is. Ontwerp van de veiligheid ziet er goed uit. Nieuwe toepassingen van derden worden ontsloten. Aanbevolen wordt deze toepassingen te testen.

4.6.6 Samenvatting

Inleiding: Antwoordvoorbedrijven is een informatieve website die ondernemers wegwijs maakt door de grote hoeveelheid van informatie van de overheid.
Risicoprofiel van de dienst: Antwoordvoorbedrijven is een informatieve website met publieke informatie voor ondernemers.Antwoordvoorbedrijven bevat en verwerkt geen gevoelige gegevens of

persoonsgegevens en heeft geen rol in de afhandeling van transacties van en met de overheid. Als de site enkele dagen tot een week niet beschikbaar is, is de impact laag. Hoewel er geen bijzondere eisen gesteld worden aan de veiligheid van de gepresenteerde gegevens, is het wenselijk dat de integriteit van de gegevens geborgd is.

Is het ontwerp van de elektronische dienst veilig?

Risicoanalyse(s) aanwezig? TNO heeft in maart 2011 een risicoanalyse uitgevoerd. Hierin wordt geconcludeerd dat de onbeschikbaarheid van de site geen grote impact heeft. Destijds was de aanbeveling om Berichtenbox benaderbaar te maken als Antwoordvoorbedrijven niet beschikbaar is. Geïnterviewden gaven aan dat dit inmiddels een eis is en geregeld is. Verder worden nog mogelijke risico's op basis van softwarefouten benoemd. Na review van de softwarecode en het herstellen van de gevonden fouten is dit opgelost. Het vinden en herstellen van toekomstige fouten is nog niet procesmatig geborgd.

Is de feitelijke werking van de elektronische dienst veilig?

Antwoordvoorbedrijven is een eenvoudige website. Regelmatige penetratietesten van de website geven aan dat het gerealiseerde beveiligingsniveau voldoende is. Bovendien wordt daarmee ook het beveiligingsniveau in de toekomst voldoende getoetst. Gezien het lage beveiligingsniveau dat nodig is voor Antwoordvoorbedrijven is geen verder onderzoek gedaan naar de beheer- en beveiligingsprocessen achter de beveiligingsmaatregelen.

Oordeel:

Antwoordvoorbedrijven inclusief Ondernemersplatform en Open Data heeft voldoende aandacht voor veiligheid in de vorm van testen, ontwerpen en Threat and Vulnerability Analysis (TVA's).

Aanbevelingen:

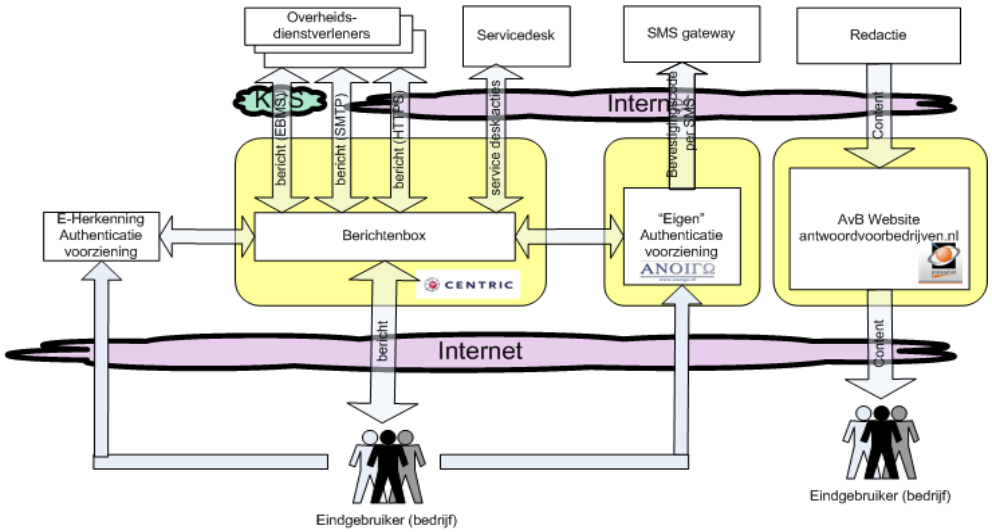
- Houdt veiligheid goed op de agenda van Antwoordvoorbedrijven.
- Het Ondernemersplatform is een portal omgeving binnen Antwoordvoorbedrijven die in ontwikkeling is en in bètaversie beschikbaar. Het ontwerp van de veiligheid ziet er goed uit. Nieuwe toepassingen van derden worden ontsloten. Aanbevolen wordt deze toepassingen te testen.

4.7 Berichtenbox

4.7.1 Korte beschrijving

De Berichtenbox voor Bedrijven (BBvB) maakt organisatorisch onderdeel uit van Antwoordvoorbedrijven maar is in dit onderzoek apart behandeld. BBvB is ingericht om te voldoen aan de Europese Dienstenrichtlijn en de daaruit voortvloeiende Nederlandse Dienstenwet. Via BBvB kunnen bedrijven op een betrouwbare manier communiceren met de overheid voor zaken die onder de Dienstenwet vallen. BBvB zorgt onder meer voor gegarandeerde aflevering van berichten, voorkomt onderscheppen van berichten tijdens transport en garandeert richting bedrijven de authenticiteit van de bevoegde instanties in de communicatie.

Ongeveer 600 overheidsinstantes zijn op BBvB aangesloten, waaronder alle gemeenten, provincies en waterschappen. Er zijn ongeveer 800 bedrijven die een berichtenbox hebben. Het aantal berichten dat met BBvB verstuurd wordt, is gering (ongeveer 2035 berichten in 2010).

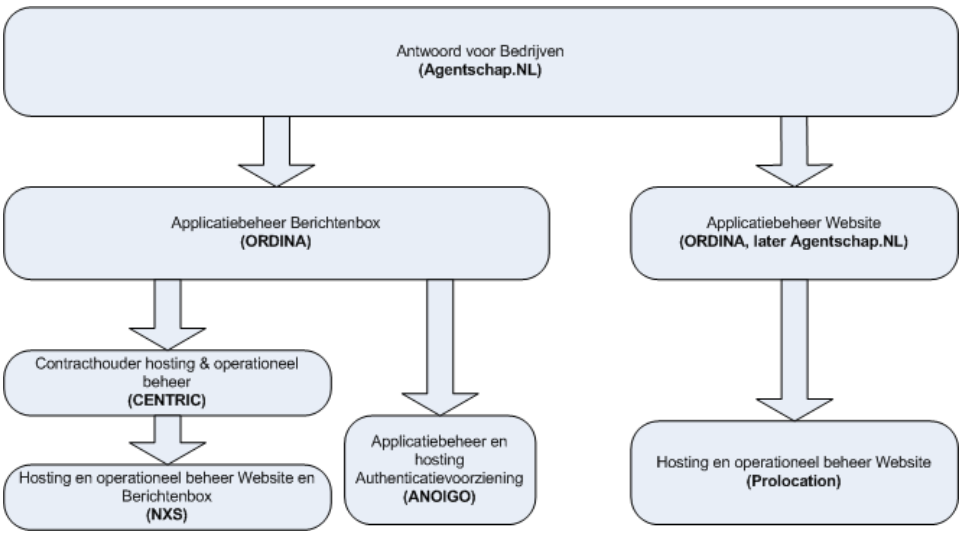


Figuur 7: Schematisch overzicht Berichtenbox

BBvB bestaat uit een berichtenboxsysteem en een 'eigen'authenticatiesysteem. Toegang tot de berichtenboxen is mogelijk via dit authenticatiesysteem, of via eHerkenning. Bij registratie in het eigen authenticatiesysteem wordt geen identiteitscontrole uitgevoerd. Dit wordt niet nodig geacht omdat de plicht tot identificatie (en de mate waarin) ligt bij de bevoegde instantie, en erg afhankelijk is van de betreffende procedure. Wel is door de registratie zoveel mogelijk zeker gesteld dat uitsluitend degene die de berichtenbox heeft aangemaakt en door hem / haar geautoriseerde personen toegang hebben tot de betreffende berichtenbox.
Bij eHerkenning vindt wel een vorm van identificatie plaats bij registratie, afhankelijk van het eHerkenningsniveau. Wanneer binnen BBvB gebruik gemaakt wordt van eHerkenning, wordt per bericht identificerende informatie (het KvK nummer) meegestuurd naar de bevoegde instantie. Identificerende informatie kan ook worden meegestuurd indien een andere geschikte vorm van

authenticatie wordt gebruikt, bijvoorbeeld een gekwalificeerd certificaat (dit kan het geval zijn bij een gebruiker van een bedrijf gevestigd in een andere lidstaat dat niet aan eHerkenning deelneemt). Dit voorkomt dat Nederlandse bedrijven worden bevoordeeld. Dit voorkomt dat Nederlandse bedrijven worden bevoordeeld op buitenlandse (die nog geen eHerkenning kunnen gebruiken) op basis van de gekozen oplossing voor authenticatie.
Wet- en regelgeving bepalen wanneer bevoegde instanties een authenticatiemethode (of beter gezegd een elektronische handtekening) moeten kunnen accepteren indien het gaat om ondertekening van berichten die via de BBvB worden verzonden.

Twee partijen (OLO en NOvA) maken gebruik van een geautomatiseerde SMTP-koppeling (Simple Mail Transfer Protocol, internationale standaard) voor het benaderen van hun berichtenbox. De andere overheidsdienstverleners loggen handmatig in met gebruik van username-password. Naast de SMTP-koppeling is Digikoppeling beschikbaar als geautomatiseerde koppeling. Hiervan zal binnenkort door de Kamer van Koophandel gebruik gemaakt gaan worden. Het is de bedoeling dat de SMTP-koppeling op termijn uitgefaseerd wordt.



Figuur 8: Overzicht beheer en hosting Berichtenbox

BBvB is in opdracht van het ministerie van Economische Zaken ontwikkeld bij ICTU en sinds eind 2009 operationeel. Begin 2011 is het beheer van BBvB overgegaan van ICTU naar Agentschap NL (AGNL). Het was aanvankelijk de bedoeling dat beheer van BBvB naar Logius zou gaan, maar dit was in 2011 niet mogelijk. Wel bestond tot kort geleden de verwachting dat BBvB per begin 2012 over zou gaan naar Logius. Het is inmiddels echter duidelijk geworden dat dit in 2012 niet zal gebeuren, mede vanwege het mogelijke samengaan met de berichtenbox voor burgers. BBvB blijft ook in 2012 onder beheer van Agentschap NL.

Regie over operationeel beheer van het berichtenboxsysteem en het authenticatiesysteem is belegd bij Ordina. Ordina coördineert wijzigingen en bewaakt het behalen van service levels. Ordina rapporteert maandelijks aan Agentschap NL en overlegt maandelijks met Agentschap NL. Bij voorbereiding van een nieuwe release is dit overleg tweewekelijks. Applicatiebeheer van het berichtenboxsysteem is belegd bij Ordina. Hosting van het berichtenboxsysteem is belegd bij Centric/NXS. Applicatiebeheer en hosting

van het authenticatiesysteem is belegd bij Anoigo. De Servicedesk is belegd bij Logius. Agentschap NL heeft met alle partijen (behalve NXS) zelf de contracten afgesloten.

Status	Operationeel sinds 2009 en momenteel in tijdelijke beheerfase
Eigenaar	Ministerie van EL&I
Functioneel beheer	Agentschap NL
Applicatiebeheer	Ordina (berichtenbox + coördinatie) en Anoigo (authenticatiedienst)
Technisch beheer	Centic/NXS (berichtenbox) en Anoigo (authenticatiedienst)

4.7.2 Risicoprofiel

BBvB is bedoeld voor betrouwbare communicatie met de overheid. Dit stijgt uit boven het niveau van normale e-mail uitwisseling. Daarom stelt BBvB zeer hoge eisen op het gebied van vertrouwelijkheid en integriteit en hoge eisen waar het gaat om beschikbaarheid. Dit komt overeen met de resultaten van de Business Impact Assessment (BIA) uit 2010. In de Business Impact Assessment is bepaald dat de maximaal toegestane (aaneengesloten) uitvalsduur (MTU) 2-3 dagen is.

Naast de directe gevolgen door incidenten met betrekking tot BBvB, bestaat voor alle deelnemende partijen en met name voor de 'eigenaar', het Ministerie van EL&I, de reële mogelijkheid van imagoschade.

Binnen BBvB worden persoonsgegevens verwerkt. Hiervoor is de Wbp (wet bescherming persoonsgegevens) van toepassing. Voor BBvB geldt dat voor het beheer van de geregistreerde persoonsgegevens een beveiligingsniveau dat voldoet aan Wbp risicoklasse 2 volstaat. Dit is vastgelegd in het tactisch beveiligingsplan.

Veiligheidsaspect	Vereist beveiligingsniveau
Beschikbaarheid	Hoog
Integriteit	Zeer hoog
Vertrouwelijkheid	Zeer hoog
Maximaal Toegestane Uitval (MTU)	2-3 dagen

4.7.3 Bevindingen

Algemeen
De huidige beheerorganisatie (Agentschap NL) ziet zichzelf als een tijdelijke beheerorganisatie voor BBvB, totdat voor BBvB een beheerorganisatie geregeld is die BBvB een permanenter onderdak kan bieden. Vanwege de tijdelijke huisvesting van BBvB heeft Agentschap NL de governance van het beheer en de beveiliging van BBvB beperkt ingericht. Inmiddels loopt de tijdelijke situatie echter zo ver uit dat de governance op een hoger niveau gebracht moet worden om de veiligheid te kunnen blijven garanderen.

Daarnaast is het voortbestaan van BBvB in zijn huidige vorm onzeker vanwege de intentie BBvB samen te voegen met de berichtenbox voor burgers.

Aanpassingen in de realisatie van BBvB worden overwogen, o.a. vervangen van het huidige authenticatiesysteem door de authenticatiedienst van e-loket, het op termijn volledig overgaan op authenticatie met eHerkenning en uitfasering van de SMTP-koppeling (Simple Mail Transfer Protocol, internationale standaard) t.b.v. Digikoppeling.

Beleid en standaarden
De wet- en regelgeving (Europese Dienstenrichtlijn, Dienstenwet, algemene maarregel van bestuur (AMvB) 'Dienstenbesluit centraal loket' en ministeriële regeling 'Dienstenregeling centraal loket en interne markt informatiesysteem') die op BBvB van toepassing is, is goed in kaart gebracht en er vindt vanuit het Ministerie van EL&I duidelijke sturing (begeleiding) plaats om de realisatie hieraan te laten voldoen. Gewenste wijzigingen in BBvB moeten in sommige gevallen vooraf gegaan worden door AMvB en/of ministeriële regeling.

Toezicht op BBvB is niet ingevuld.

Processen en procedures
Eind 2010 – begin 2011 is een risicoanalyse op functioneel niveau uitgevoerd. Op basis van de risicoanalyse zijn een strategisch en een tactisch informatiebeveiligingsplan opgesteld. Geen van beide bevat een calamiteitenparagraaf. Er is nog geen gap-analyse opgesteld om bij te houden in hoeverre de maatregelen uit de beveiligingsplannen geïmplementeerd zijn. De risicoanalyse en de informatiebeveiligingsplannen worden niet goed bijgehouden. Het is de bedoeling dat binnenkort aan een externe partij opdracht wordt gegeven om een calamiteitenplan op te stellen. Er zijn nog geen plannen voor een gap-analyse

Incident-, configuratie- en wijzigingsbeheer zijn vastgelegd in een "Service Niveau Overeenkomst" (SNO) tussen Agentschap NL en Ordina en Centric. Aanvullend zijn er (beperkte) detailafspraken tussen Ordina en Centric. Ook in het "Dossier Afspraken en Procedures" (DAP) wordt ingegaan op incident-, configuratie- en wijzigingsbeheer. SNO en DAP zijn zeer recent (3 november 2011).

Audits hebben nog niet plaatsgevonden. Wel wordt gewerkt aan het opzetten van een audit en het maken van afspraken over auditbezoeken bij de applicatie- en technisch beheerders.

Voor het in productie nemen van een nieuwe release vinden keten- en acceptatietesten plaats.

Techniek
Bij het ontwerp van het berichtenboxsysteem en het authenticatiesysteem is meegenomen dat de applicaties tegen de Open Web Application Security Project [OWASP] top 10 beveiligingsrisico's moeten zijn beveiligd.

Er wordt uitgebreide logging toegepast om ervoor te zorgen dat foutieve handelingen altijd terug te vinden zijn en indien nodig te reconstrueren zijn.

Jaarlijks vinden penetratietesten plaats door een professionele partij. De laatste penetratietest heeft plaatsgevonden eind 2010 door Madison Gurkha. Een nieuwe penetratietest is in voorbereiding.

In 2010 heeft een systematisch onderzoek naar computer broncode ("*Code Review*") plaatsgevonden door een professionele partij die heeft geleid tot aanpassingen in de software.

De ontwikkel-, test-, acceptatie- en productieomgeving zijn van elkaar gescheiden. De ontwikkel- en testomgeving bevinden zich bij een andere partij dan de acceptatie- en productieomgeving.

4.7.4 Oordeel

Algemeen
Voor nu is de berichtenbox technisch veilig op grond van de gedane penetratietesten en *code review*. Aandacht voor de veiligheid dient direct te worden aangescherpt, nu duidelijk is dat de Berichtenbox in elk geval in 2012 operationeel blijft.D e huidige beheerorganisatie is een tijdelijke. Aangezien de overdracht naar een permanente oplossing al enkele keren uitgesteld is, is meer aandacht nodig voor de governance voor BBvB. De huidige beheerorganisatie heeft de governance voor BBvB niet voldoende op orde. Daarnaast is er nog veel onduidelijk over de toekomst van BBvB.

Beleid en standaarden
De van toepassing zijnde wet- en regelgeving is duidelijk.

De besturings-, beheer en beveiligingsprocessen zijn niet voldoende uitgewerkt. Hierdoor kunnen noodzakelijke beveiligingsmaatregelen over het hoofd gezien worden.

Processen en procedures
De risicoanalyse en de informatiebeveiligingsplannen zijn initieel wel opgesteld, maar worden niet goed bijgehouden. Er is nog geen calamiteitenplan. Verder is er geen gap-analyse, waardoor het onduidelijk is in hoeverre de benodigde maatregelen geïmplementeerd zijn.

De belangrijkste beheerprocessen zijn op afsprakenniveau ingericht, maar door het ontbreken van audits is er geen duidelijkheid over de kwaliteit en het naleven van de procedures en beveiligingsmaatregelen. Penetratietesten geven slechts een beperkte toetsing op het gebied van veiligheid.

Door tekortkomingen in het ontwerp van de besturing-, beheer- en beveiligingsprocessen en het ontbreken van regelmatige audits in opdracht van de eigenaar van de dienst is de veiligheid van deze dienst nu en op termijn niet geborgd.

Techniek
Er is de nodige aandacht geweest voor technische beveiligingsmaatregelen als code reviews en penetratietesten en het implementeren van de daaruit voortvloeiende verbeteringen; acties die op uitvoeringsniveau in deze situatie belangrijk bijdragen tot de veiligheid van de dienst nu.

De beheersorganisatie heeft weinig zicht op de uitvoering van beveiligingsmaatregelen door de leveranciers.

4.7.5 Aanbevelingen

Algemeen
Creëer duidelijkheid over de plannen met BBvB. De overdracht naar een permanente beheerorganisatie en het voortbestaan van BBvB zijn onduidelijk waardoor besturings-, beheer- en beveiligingsprocessen niet volledig ingericht zijn voor de tijdelijke situatie.

Beleid en standaarden
Breng de besturings-, beheer en beveiligingsprocessen op orde als BBvB is de huidige vorm nog enige tijd blijft bestaan. Voorlopig blijft BBvB in 2012 nog bij Agentschap NL en is het nodig dit aspect te verbeteren. Ondersteuning van de functioneel beheerders is daarbij gewenst.

Processen en procedures
Richt periodieke audits in om de kwaliteit en naleving van procedures en beveiligingsmaatregelen te beoordelen. Voer de audits ook uit bij de applicatie- en technisch beheerders.

Richt processen in om de risicoanalyse en het beveiligingsplan periodiek te updaten en een gap-analyse uit te voeren.

Maak vaart met het laten opstellen van een calamiteitenplan.

Techniek
Controleer de realisatie van BBvB bij de applicatie- en technisch beheerders, onder andere door reviews en audits.

4.7.6 Samenvatting

Inleiding: De Berichtenbox voor Bedrijven (BBvB) maakt organisatorisch onderdeel uit van Antwoordvoorbedrijven maar is in dit onderzoek apart behandeld. BBvB is ingericht om te voldoen aan de Europese Dienstenrichtlijn en de daaruit voortvloeiende Nederlandse Dienstenwet. Via BBvB kunnen bedrijven op een betrouwbare manier communiceren met de overheid voor zaken die onder de Dienstenwet vallen. BBvB valt onder verantwoordelijkheid van het Ministerie van EL&I. Functioneel beheer ligt bij Agenschap NL (AGNL). Het operationeel beheer is uitbesteed aan de bedrijven Ordina (o.a. regietaak), Centric/NXS en Anoigo.
Risicoprofiel van de dienst: BBvB is bedoeld voor betrouwbare communicatie met de overheid. BBvB stelt hoge eisen op het gebied van vertrouwelijkheid en integriteit en middelmatige eisen waar het gaat om beschikbaarheidVoor de dienst is bepaald dat de maximaal toegestane uitvalsduur 2-3 dagen is. Naast de directe gevolgen door incidenten met betrekking tot BBvB, bestaat voor alle deelnemende partijen en met name voor de ‘eigenaar’, het Ministerie van EL&I, de reële mogelijkheid van imagoschade.
Is het ontwerp van de elektronische dienst veilig? **Risicoanalyse aanwezig?** Eind 2010 – begin 2011 is een risicoanalyse op functioneel niveau uitgevoerd. **Veiligheid in het ontwerp geborgd?**

De risicoanalyse en de informatiebeveiligingsplannen worden niet goed bijgehouden. Er is nog geen gap-analyse opgesteld om bij te houden in hoeverre de maatregelen uit de beveiligingsplannen geïmplementeerd zijn. De beveiligingsplannen bevatten geen calamiteitenparagraaf.
Bij het ontwerp is uitgegaan van het beperken van de beveiligingsrisico's die gedefinieerd zijn in de standaard "Open Web Application Security Project". Er heeft een review van de softwarecode plaatsgevonden in 2010 die heeft geleid tot aanpassingen in de software.

Veiligheid in de beheerfase geborgd?
Met de operationeel beheerders zijn afspraken vastgelegd over incident-, probleem- en wijzigingsbeheer.

Risico's voldoende afgedekt?
De besturings-, beheer en beveiligingsprocessen zijn niet voldoende uitgewerkt. Hierdoor kunnen noodzakelijke beveiligingsmaatregelen over het hoofd gezien worden.

Is de feitelijke werking van de elektronische dienst veilig?

Worden de veiligheidsmaatregelen uitgevoerd zowel in de front- als de backoffice?
De belangrijkste beheerprocessen zijn op afsprakenniveau ingericht, maar door het ontbreken van audits is er geen duidelijkheid over de kwaliteit en het naleven van de procedures en beveiligingsmaatregelen.

Wie controleert dit?
Er hebben tot nog toe geen audits plaatsgevonden. Jaarlijks wordt een penetratietest gedaan door een externe partij.

Risico's voldoende afgedekt?
Er is de nodige aandacht geweest voor technische beveiligingsmaatregelen als *code reviews* en penetratietesten en het implementeren van de daaruit voortvloeiende verbeteringen; acties die op uitvoeringsniveau in deze situatie belangrijk bijdragen tot de veiligheid van de dienst nu.

Op dit moment is niet duidelijk of beoogde beveiligingsmaatregelen door de leveranciers in de praktijk uitgevoerd en nageleefd worden.

Oordeel:
Voor nu is de berichtenbox technisch veilig. Op uitvoeringsniveau zijn acties (*code reviews*[10] en penetratietesten) uitgevoerd en opgevolgd om de veiligheid te bevorderen. Echter het ontwerp van de de besturing-, beheer en beveiligingsprocessen is niet voldoende uitgewerkt waardoor de veiligheid niet structureel is geborgd. Structurele aandacht voor de veiligheid dient te worden geborgd nu duidelijk is dat de Berichtenbox in elk geval in 2012 operationeel blijft. Doordat het ontwerp van de besturing-, beheer en beveiligingsprocessen niet voldoende is uitgewerkt zijn mogelijk noodzakelijke beveiligingsmaatregelen over het hoofd gezien. De implementatie van de processen en maatregelen uit het ontwerp is nog niet getoetst door middel van een audit. Daardoor is het onduidelijk in hoeverre de implementatie is afgerond. De mogelijke tekortkomingen in het ontwerp van de besturing-, beheer- en beveiligingsprocessen en het ontbreken van regelmatige audits in opdracht van de eigenaar van de dienst dienen met spoed te worden opgepakt om de veiligheid van deze dienst op korte termijn al sterk te verbeteren en te borgen.

Aanbevelingen:

[10] Code reviews: systematisch onderzoek naar broncode van software programma's

- Breng de besturings-, beheer en beveiligingsprocessen op orde nu duidelijk is dat BBvB in 2012 nog bij Agentschap NL blijft.
- Richt als EL&Iperiodieke audits in om de kwaliteit en naleving van procedures en beveiligingsmaatregelen te beoordelen die ook de applicatie- en technisch beheerders meenemen in het onderzoek. Zorg dat deze audit zich niet beperkt tot een review van bestaande auditrapporten van de applicatie- en technisch beheerders. Zorg dat de audits een inhoudelijke toetsing omvatten van de risico- en gap-analyses.
- Richt processen in om de risicoanalyse en het beveiligingsplan periodiek te updaten en een gap-analyse uit te voeren. Maak vaart met het laten opstellen van een calamiteitenplan.

5 CONCLUSIE

In opdracht van het Ministerie van EL&I is de veiligheid onderzocht van de volgende negen diensten uit de Digitale Agenda.nl: Regelhulp, OndernemingsDossier, Standaard Bedrijfsrapportage (SBR), eFactureren, eHerkenning, Antwoordvoorbedrijven, Ondernemersplatform, Open Data en Berichtenbox. Tevens is de voor SBR en eFactureren noodzakelijke dienst Digipoort-PI in het onderzoek meegenomen. Regelhulp is in overleg met de opdrachtgever buiten scope geplaatst, omdat er nog geen ontwerp of werkend systeem “Regelhulp voor bedrijven” is.

De negen diensten zijn: Regelhulp, OndernemingsDossier, Standaard Bedrijfsrapportage (SBR), eFactureren, eHerkenning, Antwoordvoorbedrijven, Ondernemersplatform, Open Data en Berichtenbox. Regelhulp is in overleg met de opdrachtgever buiten scope geplaatst, omdat er nog geen ontwerp of werkend systeem . De voor SBR en eFactureren noodzakelijke dienst Digipoort-PI is in het onderzoek meegenomen.

De vragen, die het Ministerie van EL&I beantwoord wilde zien door middel van het onderzoek, zijn:

A. Is het ontwerp (inrichting, proces en beheer) van de elektronische overheidsdiensten die beschreven zijn in de Digitale Agenda.nl veilig?
    1. Is er een risicoanalyse gemaakt?
    2. Welke maatregelen zijn er in het ontwerp van de diensten genomen om veiligheid te borgen?
    3. Welke maatregelen zijn of worden in de beheerfase van de diensten genomen om de veiligheid te borgen?
    4. Dekken de maatregelen de risico’s voldoende af, c.q. is de risicoanalyse betrouwbaar?
B. Is de feitelijke werking van de diensten veilig?
    1. Worden de maatregelen in het ontwerp en de beheerfase van de diensten in de praktijk uitgevoerd door betrokken stakeholders en zowel in de front- als de backoffice (voor zover de dienst reeds operationeel is) en wie controleert dit?
    2. Dekken de maatregelen de risico’s voldoende af, c.q. is de risicoanalyse betrouwbaar, c.q. vragen operationele tekortkomingen om aanvullende maatregelen?

Clustering

In het onderzoek zijn enkele diensten geclusterd of apart benoemd. Antwoordvoorbedrijven is in het onderzoek geclusterd met Ondernemersplatform en Open Data vanuit het oogpunt van verwantschap. SBR en eFactureren maken samen gebruik van een voor de dienst essentiële infrastructuur Digipoort-PI en zijn tevens geclusterd. Berichtenbox is organisatorisch ondergebracht bij Antwoordvoorbedrijven, maar wordt in dit onderzoek apart behandeld onder Berichtenbox.

Beoordeling per dienst / cluster diensten in het kort

De kort samengevatte beoordeling per dienst, of cluster van diensten, is als volgt:

- **OndernemingsDossier:** In het huidige beginstadium lijkt het OndernemingsDossier veilig, zoals uitgevoerd onder de verantwoordelijkheid van de initiatiefnemende branches. Een integrale governance met duidelijke veiligheidsparagraaf voor de samenwerking tussen overheid en het bedrijfsleven is noodzakelijk voor verder groei van het ondernemingsdossier. Hierin moet bijvoorbeeld de vraag worden beantwoord wie onderzoek gaat uitvoeren naar en eisen moet stellen aan de veiligheid van een ondernemingsdossier. De verantwoordelijkheden van EL&I en private marktpartijen dienen expliciet te worden gemaakt.

- **Cluster Standaard Bedrijfsrapportage (SBR) en eFactureren, inclusief Digipoort-PI:** Voor Digipoort-PI zijn veiligheid en beheer goed geregeld. SBR en eFactureren zijn afsprakenstelsels. Voor SBR en eFactureren is het eigenaarschap niet goed uitgekristalliseerd, maar de veiligheid is niet direct in het geding. De risico's voor SBR en eFactureren, voor zover deze betrekking hebben veiligheid, vallen binnen Digipoort-PI.
- **eHerkenning**: Het ontwerp van de besturing-, beheer- en beveiligingsprocessen op stelselniveau is voor de transitiefase voldoende veilig, zij het niet overtuigend. Aanvullende zekerstelling is gewenst, met name door onafhankelijke review van de risicoanalyses en het bepalen of op stelselniveau aanvullende eisen op het gebied van informatiebeveiliging nodig zijn. Daarnaast zou er vaart gemaakt moeten worden met de transitie naar de definitieve beheerfase bij Logius. De ontworpen (deels tijdelijke) processen en de maatregelen uit het normenkader lijken op deelnemer- en stelselniveau goed geïmplementeerd te zijn, maar er vindt onvoldoende monitoring plaats op het implementeren van wijzigingen en nieuwe maatregelen. Dit kan leiden tot incidenten op het gebied van veiligheid. Voor de borging van de veiligheid op termijn is het nodig om het ontwerp van de processen op stelselniveau te verbeteren, het implementeren van wijzigingen en nieuwe maatregelen effectief te monitoren en regelmatig een uitgebreide stelselaudit uit te voeren in opdracht van de beleidsopdrachtgever van eHerkenning.
- **Cluster Antwoordvoorbedrijven (inclusief Ondernemersplatform en Open Data)**: Cluster Antwoordvoorbedrijven heeft voldoende aandacht voor veiligheid in de vorm van testen, ontwerpen en Threat and Vulnerability Analysis (TVA's).
- **Berichtenbox (BBvB)**: Voor nu is de berichtenbox technisch veilig. Op uitvoeringsniveau zijn acties (*code reviews*[11] en penetratietesten) uitgevoerd en opgevolgd om de veiligheid te bevorderen. Echter het ontwerp van de de besturing-, beheer en beveiligingsprocessen is niet voldoende uitgewerkt waardoor de veiligheid niet structureel is geborgd. Structurele aandacht voor de veiligheid dient te worden geborgd nu duidelijk is dat de Berichtenbox in elk geval in 2012 operationeel blijft. Doordat het ontwerp van de besturing-, beheer en beveiligingsprocessen niet voldoende is uitgewerkt zijn mogelijk noodzakelijke beveiligingsmaatregelen over het hoofd gezien. De implementatie van de processen en maatregelen uit het ontwerp is nog niet getoetst door middel van een audit. Daardoor is het onduidelijk in hoeverre de implementatie is afgerond. De mogelijke tekortkomingen in het ontwerp van de besturing-, beheer- en beveiligingsprocessen en het ontbreken van regelmatige audits in opdracht van de eigenaar van de dienst dienen met spoed te worden opgepakt om de veiligheid van deze dienst op korte termijn al sterk te verbeteren en te borgen.

Is het ontwerp van de diensten veilig?

Bij de drie diensten die hoge eisen stellen op het gebied van veiligheid, is het aspect veiligheid (eHerkenning, Berichtenbox en Digipoort-PI) een belangrijk criterium geweest in het o*ntwerp van d*e dienst en het beheer ervan. Bij Digipoort-PI heeft dit geleid tot een veilige dienst. Bij eHerkenning en Berichtenbox zijn er onvolkomenheden op het gebied van governance en continuïteit van de beheerorganisatie. Daarnaast ontbreken in het ontwerp van deze twee diensten een aantal beveiligingsmaatregelen dat de veiligheid van deze diensten op termijn verbetert. Ten tijde van het onderzoek was eHerkenning voldoende veilig, maar niet overtuigend. Door de genoemde onvolkomenheden kan voor de langere termijn geen veilige werking gegarandeerd worden. Voor Berichtenbox is het van belang op korte termijn vast te stellen of dit het geval is door het uitvoeren van een gap analyse en controle bij de uitvoerende partijen.

[11] Code reviews: systematisch onderzoek naar broncode van software programma's

Bij de diensten die lage tot middelmatige eisen stellen, krijgt beveiliging in het ontwerp van de dienst en het beheer ervan minder aandacht, maar dat is ook reëel en het beoogde beveiligingsniveau is voor deze diensten voldoende.

Bij iedere dienst is een restrisico aanwezig. Het is namelijk niet haalbaar en niet betaalbaar om de risico's voor de dienst tot nul te reduceren. De eigenaar van de dienst bepaalt welke kosten voor het beveiligen van de dienst nog redelijk zijn, en daarmee welk restrisico acceptabel is. Dit betekent echter dat bij het volledig en correct implementeren en uitvoeren van alle beoogde beveiligingsmaatregelen, toch een beveiligingsincident op kan treden. Het restrisico voor de dienst moet bewust geaccepteerd en vastgelegd worden door de eigenaar van de dienst. Voor geen van de onderzochte diensten, behalve Digipoort-PI, is echter het restrisico bepaald, geaccepteerd en vastgelegd door de eigenaar ervan.

Is de feitelijke werking veilig?
Bij alle operationele diensten zijn de beoogde beveiligingsmaatregelen getroffen, maar niet voor alle diensten wordt dit goed gemonitoord. Alleen voor Digipoort-PI is er afdoende monitoring op het implementeren van beveiligingsmaatregelen. Onzorgvuldigheid bij de naleving van beveiligingsmaatregelen kan al op korte termijn tot incidenten leiden. De aanbeveling is om op korte termijn te investeren in het beter monitoren van het implementeren van beveiligingsmaatregelen. Daarnaast is voor Berichtenbox op korte termijn een audit op de kwaliteit en het naleven van de procedures en beveiligingsmaatregelen noodzakelijk.

Om de veiligheid van de diensten op termijn zeker te kunnen blijven stellen, zijn verbeteringen en uniformering in auditing en aanvullende technische maatregelen nodig. Voor wat betreft de veiligheid van de diensten is er geen overheidstoezicht vanwege het ontbreken van een wettelijk kader hiervoor. De beleidsverantwoordelijken hebben gekozen voor controle via auditing. Voor alle operationele diensten wordt gebruik gemaakt van auditing (behalve bij Berichtenbox) en penetratietesten. Bij auditing wordt echter te veel vertrouwd op audits waarvan de onderzoekers vinden dat de uitvoerders van de diensten de scope en diepgang van de audits te veel zelf kunnen beïnvloeden. Dit is vooral een aandachtspunt voor de diensten die hoge eisen stellen op het gebied van veiligheid (eHerkenning, Berichtenbox en Digipoort-PI). Het uitgangspunt zou dan ook moeten zijn dat voor deze diensten de opdrachtgever van de dienst, de scope en diepte voor de audits bepaalt.

Bij penetratietesten wordt te veel vertrouwd op de volledigheid van deze testen. Penetratietesten geven echter een beperkte toetsing op het gebied van veiligheid. Penetratietesten zijn bedoeld als aanvulling op andere beveiliging- en toetsingsmaatregelen. De beheerders van diensten die hoge eisen stellen op het gebied van veiligheid (eHerkenning, Berichtenbox en Digipoort-PI) zouden moeten overwegen om meer gebruik te maken van systemen die hackers kunnen detecteren en andere proactieve technische maatregelen om operationele risico's te verkleinen.

Verantwoording onderzoek
De onderzoekers hebben in hun onderzoek naar het ontwerp en de feitelijke werking van de veiligheid van de diensten in de Digitale Agenda.nl de risicoprofielen meegewogen in de diepte van het onderzoek. Daar waar de onderzoekers het noodzakelijk vonden is aanvullende documentatie op locatie ingezien en zijn bijvoorbeeld certificaten gecontroleerd. Daarnaast bleek tijdens het onderzoek dat bij de meeste diensten recent audits en penetratietesten waren uitgevoerd. Er is voor gekozen deze niet opnieuw uit te voeren. Bij private partijen zijn geen controles gedaan.

6 REFERENTIES

In de tabel hieronder een overzicht van referenties. De documenten ontvangen van de verschillende diensten zijn in de appendix per dienst opgenomen.

Referentie	Document
[DigitaleAgenda]	Digitale Agenda.nl, http://www.rijksoverheid.nl/documenten-en-publicaties/notas/2011/05/17/digitale-agenda-nl-ict-voor-innovatie-en-economische-groei.html
[ISO27001]	ISO/IEC 27001 standard
[ISO27002]	ISO/IEC 27002 standard
[Kamerbrief]	Donner, J.P.H., Opstelten, I.W., *Kamerbrief Digitale Inbraak Diginotar*, 15 september 2011
[KickOff]	Van Dam, H.J., P.J.M. Hin, M. Radema, *Kick-off en afspraken Onderzoek Veiligheid Diensten in de Digitale Agenda.nl*, 28 oktober 2011
[NORA]	Van der Veen, J., Bokhorst, B., *NORA Dossier Informatiebeveiliging: Normen IT-voorzieningen*, 1 september 2010, versie 1.3
[Offerte]	Collis, *Onderzoek veiligheid diensten in Digitale Agenda.nl*, 18 oktober 2011
[Opdracht]	Kroon, L.M.N.,*Offerteaavraag onderzoek veiligheid diensten in Digitale Agenda.nl*,
[OWASP]	Zie www.owasp.com
[Regelhulp]	ATLAS-#11083433-v2-Offerteaanvraag_BMC_Positionering_Regelhulp, 20 juni 2011
[SNO Digipoort-PI]	Serviceniveau Overeenkomst Digipoort X400, SMTP, FTP, POP3, SOAP, WUS en EbMS Versie 1.02, 16 november 2010
[STORK]	Secure Identity Across Borders Linked, Framework Programme, https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312
[STORKQAS]	STORK, *D2.3 - Quality Authenticator Scheme*, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577
[VIR]	Voorschrift Informatiebeveiliging Rijksdienst, http://wetten.overheid.nl/BWBR0022141
[Wbp]	Wet bescherming persoonsgegevens, http://wetten.overheid.nl/BWBR0011468

APPENDICES

App 1 INITIEEL OPGEVRAAGDE DOCUMENTATIE

E-mail verstuurd aan Geert Jan Visser, 28/10/2011 16.05

Aan de dossierhouders van 9 diensten van de Digitale Agenda.nl

In opdracht van directeur regeldruk & ICT beleid i.o. van het Ministerie van EL&I wordt een onderzoek uitgevoerd veiligheid diensten Digitale Agenda.nl. Dit onderzoek behelst een onderzoek naar 9 diensten in de Digitale Agenda.nl. Het onderzoek wordt uitgevoerd door de combinatie Collis / HEC (zie voor de bedrijfsprofielen www.collis.nl en www.hec.nl.)

De uitvraag van het onderzoek heeft als kenmerk ETM/IP/11146588. In de bijlage van deze brief zijn de onderzoeksvragen geformuleerd.

Met Ir. G.J. Visser, Beleidsadviseur/plv. secretaris DGBI is afgesproken dat de initiële informatievraag aan u via hem verloopt. Sommige diensten hebben reeds informatie beschikbaar gesteld.

Om het onderzoek uit te voeren heeft Collis/HEC gegevens van de dienst waar u dossierhouder van bent nodig. De hoofdvragen en subvragen van het onderzoek zijn:

- Is het ontwerp (inrichting, proces en beheer) van de elektronische overheidsdiensten die beschreven zijn in de Digitale Agenda.nl veilig?
  - Is er een risicoanalyse gemaakt?
  - Welke maatregelen zijn er in het ontwerp van de diensten genomen om veiligheid te borgen?
  - Welke maatregelen zijn of worden in de beheerfase van de diensten genomen om de veiligheid te borgen?
  - Dekken de maatregelen de risico's voldoende af, c.q. is de risicoanalyse betrouwbaar?
- Is de feitelijke werking van de diensten veilig?
  - Worden de maatregelen in het ontwerp en de beheerfase van de diensten in de praktijk uitgevoerd door betrokken stakeholders en zowel in de front- als de backoffice (voor zover de dienst reeds operationeel is) en wie controleert dit?
  - Dekken de maatregelen de risico's voldoende af, c.q. vragen operationele tekortkomingen om aanvullende maatregelen?

Om deze hoofdvragen te beantwoorden vragen we u informatie aan te leveren die ons hierin inzicht geeft. We denken daarbij specifiek aan:

1. De risico analyses
2. De genomen maatregelen bij ontwerp
3. De genomen maatregelen in de beheersfase, inclusief audits en andere controles
4. De belegging van de verantwoordelijkheden binnen de dienst, inclusief functioneel en operationeel beheer
5. Informatie die u – in het licht van het onderzoek - relevant acht
6. Informatie die de dienst beschrijft, zoals ontwerp en ontwikkeldocumentatie, gekozen architectuur, .., ten behoeve van ons inzicht in de dienst

Vanwege de beperkte tijd die het onderzoek loopt, de concept rapportage moet 18 november gereed zijn, dient de informatie spoedig te worden ontvangen. Tevens willen we op korte termijn een gesprek met de dossierhouder van de dienst en een persoon / meerdere personen die is aangewezen door de dossierhouder en kennis heeft omtrent de risico analyse, de genomen maatregelen en met name de genomen maatregelen in de uitvoering. De planning is als volgt:

- De gevraagde informatie dient maandag 31 en dinsdag 1 november te worden geleverd aan Geert Jan Visser.
- Het eerste gesprek met de dossierhouder (of aangewezen persoon) van de dienst vindt plaats op donderdag 3 november (bijvoorkeur op locatie Bezuidenhoutseweg 20)

Verder vraag ik u

- Uw naam, email adres en telefoonnummer door te geven
- Idem van aanvullende personen
- Uw gezamenlijke beschikbaarheid op donderdag 3 november. We proberen daar zo veel als mogelijk rekening mee te houden.

Als u vragen heeft kunt u contact met mij opnemen, of met Geert Jan Visser.

App 2 SELECTIE VAN STANDAARDEN OP GEBIED VAN INFORMATIEVOORZIENING

Hieronder een inventarisatie van verschillende standaarden binnen de NL overheid, waarbij door ons een voorselectie is gedaan op relevantie. Van deze standaarden is gebruik gemaakt bij het opstellen van het Risico- en Beoordelingskader zoals beschreven in Hoofdstuk 3.

Gebruikte afkortingen
V == Verplicht en CoE == Comply or Explain.

App 2.1 Architectuurstandaarden

Overheidsbrede standaarden

- *CoE: De NORA als referentie architectuur voor de overheid* (College Standaardisatie besluit)
  Interdepartementaal is afgesproken de NORA (Nederlandse Overheid Referentie Architectuur) voor de opbouw van de informatievoorziening als uitgangspunt te hanteren.
- *CoE: De MARIJ als architectuur voor de Rijksoverheid* (DG OBR besluit)
  DGOBR heeft de departementen aangegeven bij de ontwikkeling van een eigen departementale architectuur de MARIJ te gebruiken als norm (noot: het werkingsgebied is het kerndepartement).

App 2.2 Informatie-architectuur standaarden

E-toegang

- *V: De Webrichtlijnen* (College Standaardisatie besluit)
  Overheidswebsites dienen toegankelijk te zijn voor alle burgers en organisaties in Nederland. Binnen Nederland is dit vastgelegd in de Webrichtlijnen (zie www.webrichtlijnen.nl)

E-identificatie en E-authenticatie

- *V:Identity Management (DG OBR besluit)*
  Interdepartementaal is de afspraak gemaakt om op eenduidige wijze relevante attributen van alle overheidsmedewerkers (intern en extern) in één centraal informatiesysteem (Identity Store - Identity Management)) te verzamelen, synchroniseren en ter beschikking te stellen, bijvoorbeeld aan de sectorale Active Directories (AD), de Justitie Adressengids en Rijksweb. Bronsystemen, zoals het HRM systeem (P-direct, Planon), leveren de informatie aan de Identity Store. Hiervoor is afgesproken dat Rijksbreed het Gemeenschappelijke normenkader Rijksoverheidbreed identity management idm componenten 1 t/m 4 geldt.
  Deze standaard is verplicht voor alle Rijksoverheden.

E-Informatie uitwisseling

- *CoE: Digikoppeling* (College Standaardisatie besluit)
  Voor de uitwisseling van berichten tussen organisaties over de verschillende overheidssectoren heen, moet gebruik gemaakt worden van de protocollen uit Digikoppeling.

App 2.3 Bedrijfsarchitectuur standaarden

- *V: Archiefstandaarden* (Bestuurlijke richtlijn) Archiefbesluit, de drie ministeriële regelingen, de ISO norm 15489 en de NEN 2082. De Baseline betreft de organisatorische en functionele voorschriften voor de informatiehuishouding.

App 2.4 Standaard op het gebied van beheer

- CoE: *ITIL als technische IT beheerstandaard*
  ITIL als beheermethode voor de technische infrastructuur

App 2.5 Informatiebeveiliging standaarden

Overheidsbrede richtlijnen op het gebied van Informatiebeveiliging

- *V: Wbp* De belangrijkste regels voor het vastleggen en gebruiken van persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens
- *V: Wet elektronische handtekening:* Deze wet is de implementatie van de Europese richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen
- *V: Wet elektronisch bestuurlijk verkeer:* Deze wet bevat de regels voor het verkeer langs elektronische weg tussen burgers/bedrijven en bestuursorganen en tussen bestuursorganen onderling (de zogenaamde Wet Elektronisch Bestuurlijk Verkeer, hierna te noemen: WEBV).
- *V: VIR* Het Voorschrift Informatiebeveiliging Rijksdienst (VIR), in 2007 geheel herzien, geldt als verplicht voor de gehele Rijksoverheid
- *V: VIR BI* Voorschrift Informatiebeveiliging Rijksdienst, bijzondere informatie vastgesteld in maart 2004, geldt als verplicht voor de gehele Rijksoverheid
- *CoE: Code voor Informatiebeveiliging* (College Standaardisatie besluit)
  Deze bestaat uit de volgende normen:
  - NEN-ISO/IEC 27001:2005.nl is de specificatie van management systemen van informatiebeveiliging
  - NEN-ISO/IEC 27002:2007.nl is de set van best practices in informatiebeveiliging en dient in samenhang met de NEN-ISO/IEC 27001:2005.nl gehanteerd te worden.
- *V: PKI-Overheid* PKI voor de overheid maakt het mogelijk om elektronisch betrouwbaar te communiceren met en binnen de overheid. Op basis van de PKI voor de overheid zijn overheidsinstanties onder meer in staat e-mailberichten en documenten te ondertekenen en versleutelen. Met behulp van certificaten kunnen medewerkers en burgers betrouwbaar via Internet met de overheid en met elkaar communiceren. Speciaal daartoe aangewezen partijen geven deze certificaten (op een smartcard) uit aan personen en organisaties. (Kabinet besluit)

- *CoE: Mobiele datadragers* (DG OBR besluit)
  Het betreft een normenkader voor de Rijksdienst voor mobiele datadragers op het niveau Wbp risicoklasse 2 (zie IODI 19 april 2007). Dit niveau is ook gehanteerd bij andere normenkaders voor informatiebeveiliging (het Normenkader informatiebeveiliging Rijksweb (NIR) en het Referentiekader IB Haagse Ring). Dit niveau omvat alle VIR-informatie, zoals bedrijfsinformatie (inclusief personeelsinformatie), beleidsinformatie in ontwikkeling, wetgevingsinformatie in ontwikkeling, informatie die ook persoonsgegevens bevat (veelal in gebruik bij de uitvoeringsorganisaties / agentschappen).

App 3 CONTACTMOMENTEN EN GERAADPLEEGDE DOCUMENTATIE

Per dienst volgt een overzicht van contactmomenten en geraadpleegde documentatie.

App 3.1 Regelhulp

Geraadpleegde documentatie

Document	Auteur	Versie	Datum
Offerteaanvraag onderzoek 'Positionering Regelhulp'	L.M.N. Kroon	-	20 juni 2011
Input veiligheidsonderzoek - Regelhulp	-	-	-

Interviews en locale inspectie

Datum	Interview / lokale inspectie	Locatie	Perso(o)n(en)
20111103	Interview		E. Streefkerk, M. Sanders, R. Gooszen

App 3.2 OndernemingsDossier

Geraadpleegde documentatie

Document	Auteur	Versie	Datum
110509 ondertekende intentieverklaring	-	-	9 mei 2011
Factsheet Algemeen	-	-	9 mei 2011
Input veiligheidsonderzoek - OndernemingsDossier	-	-	-
Programma van eisen OndernemingsDossier	Projectbureau OndernemingsDossier	1.07	Augustus 2011
Referentiearchitectuur OndernemingsDossier	Projectbureau SGGV OndernemingsDossier	1.5	Juli 2011

Interviews en locale inspectie

Datum	Interview / lokale inspectie	Locatie	Perso(o)n(en)
20111103	Interview		E. Streefkerk, M. Sanders, R. Gooszen
20111111	Intverview / site visit	CPI, Oude Tonge	G.P. van 't Hoff, R. de Bruijn

App 3.3 Standaard BedrijfsRapportage (SBR) en eFactureren

Geraadpleegde documentatie

Document	Auteur	Versie	Datum
Rapportage TPM onderzoek 2010 Derde partijen EBPI en Equinix tbv Logius Digipoort	CompLions	1.0	31 december 2010
Besluit ARVODI 2011	Staatscourant	-	7 juni 2011
Aanbiedingsformulier Elekronisch factureren aan het Rijk	Minister EL&I	-	1 juli 2011
Opdrachtbrief e-Factureren 2010 (getekend)	Minister EL&I	1.2	10 september 2010
Stappenplan voor departementen voor e-bestellen en e-factureren	-	-	-
Onderbouwing gebruik Digipoort voor elektronisch factureren	R. Arendsen		14 januari 2010
Model Dienstverleningsovereenkomst ARVODI-2011	-	-	-
Besluit Aansluiting van alle ministeries op centraal aanleverpunt voor elekrtronische facturen	Minister EL&I		5 november 2010
Nota Elektronisch factureren via de Digipoort	Project e-Factureren	1.1	13 januari 2010
Prijsmodel Logius	-	-	29 juni 2010
Opdrachtverstrekking voor beheer Digipoort voor e-Facturen 2011	L.M.N. Kroon	-	8 oktober 2011
Opdrachtbrief e-factureren 2011 (getekend)	Logius	1.0	29 september 2011
Opdrachtbrief SBR 2010 (getekend)	Minister EL&I	-	17 mei 2010
Opdrachtbrief SBR 2011 (getekend)	Minister EL&I	-	29 juni 2010

Documentatie geraadpleegd op locatie

Document	Auteur	Versie	Datum
Technisch beveiligingsonderzoek Infrastructuur Digipoort PI in opdracht van logius	Madison Gurka BV	1.0	15 feb 2011
Impactanalyse Archiveren	Logius	1.0	7 april 2011
Verslag stuurgroep Digipoort-PI	Logius		11 mei 2011
Request for change detail, nummer 93424	Logius		17 okt 2011
Incident detail, nummer 122376	Logius		11 nov 2011
Functionele en niet-functionele eisen aan de basisfunctionaliteit, infrastructurele dienst	Logius	0.5	dec 2010
Procesbeschrijving OB-aangifte, niveau 0	Logius	1.0-rev	

Interviews en locale inspectie

Datum	Interview / lokale inspectie	Locatie	Perso(o)n(en)
20111103	Interview	EL&I	N. de Winne
20111115	Gesprek		J. Julianus
20111115	Gesprek		P.J.M. van der Pal
20111121	Site visit	Logius	N. de Winne, A. Hielkema
20111121	Gesprek		J. Julianus
20111121	Gesprek		P.J.M. van der Pal

App 3.4 eHerkenning

Geraadpleegde documentatie

Document	Auteur	Versie	Datum
eHerkenning – Algemene introductie	Projectbureau Afsprakenstelsel eHerkenning	1.1	17 juni 2011
eHerkenning – Informatiebeveiliging	Projectbureau Afsprakenstelsel eHerkenning	1.1	17 juni 2011
Informatiebeveiliging bij eHerkenning	M. Gerritsen, P. van der Enden.	-	26 oktober 2011
Gemeenschappelijk normenkader informatiebeveiliging eHerkenning	-	1.2	11 oktober 2011.
Notitie Penetratietesten	D. Wunderink, B. Goorkate	-	4 oktober 2011
Notitie proces incidentafhandeling	N. Damen, P van der Enden	-	29 september 2011
Toepassingsnotitie normenkader	J. van den Bosch, P. van der Enden	1.0	10 mei 2011
Risico Analyse Tijdelijke Beheer Organisatie	-	-	-
Stelselrisicoanalyse Netwerk voor eHerkenning		2.1	15 juni 2011
Agenda Bestuursvergadering Tijdelijke Beheerorganisatie, #9,13,14	-	-	15 maart, 5 juli, 18 augustus 2011
Notitie proces deelnemersovereenkomsten	Projectbureau eHerkenning	-	24 juni 2011
Notulen kernteamoverleg	N. Damen		12 april 2011
Presentatie Integrale bijeenkomst eHerkenning	M.G.H. Verhagen		12 april 2011
Notulen bijeenkomst beheer	N. Damen	-	7 juni 2011
Presentatie Beheerorganisatie eHerkenning	-	-	7 juni 2011
Email: stukken voor eHerkenning	P. van der Enden	-	11 november 2011
eHerkenning Betrouwbaarheidsniveaus	Projectbureau eHerkenning	1.1	17 juni 2011
Afsprakenstelsel eHerkenning – Service Level	Projectbureau eHerkenning	1.2	12 november 2011
Email betreffende de whitelist	P. van den Enden		21 november 2011

Documentatie geraadpleegd op lokatie

Document	Auteur	Versie	Datum
Afsprakenstelsel eHerkenning (Dit is een verzameling documenten)	Projectbureau eHerkenning	1.1	17 juni 2011
Voorstel procedure incidentafhandeling, 29 september 2011,	N. Damen, P. van der Enden		
Rapportage penetratietest eHerkenning, versie 1.0, 3 juni 2010	Fox-IT		
Overall rapport security assessment afsprakenstelsel eHerkenning, versie 1.0, 24 juni 2011	Sogeti		

Interviews en lokale inspectie

Datum	Interview / lokale inspectie	Locatie	Perso(o)n(en)
20111103	Interview	EL&I	P. van den Ende, M. Gerritsen
20111109	Site visit	ICTU, projectorg eHerkenning	P. van den Ende, I. Henneman
20111123	Gesprek	ICTU, projectorg eHerkenning	P. van der Ende, M. Gerritsen, I. Henneman

App 3.5 Antwoordvoorbedrijven inclusief Ondernemersplatform en Open Data

Geraadpleegde documentatie

Document	Auteur	Versie	Datum
ICTU142-1 Adviesrapport	Sogeti	1.1	16 mei 2011
Email Security assessment Sogeti follow up acties	L. van Riet	-	13 oktober 2011
Email Afhandeling security issues	L. van Riet	-	30 mei 2011
Tactisch Beveiligingsplan Antwoord voor Bedrijven	R. van Paassen	1.0	
Risicoanalyse TNO	Nico, Ellen	-	18 maart 2011
Risicoanalyse TNO	Nico, Josje, Ellen	-	18 maart 2011
Verslag Business Impact Assessment workshop	J. Laarakkers, R. van Paassen	-	24 september 2010
Report Threat & Vulnerability Analysis	R. van Paassen, J. Laarakkers	-	3 februari 2011
Memo Review risicoanalyse Antwoord voor Bedrijven	E. Küller, M. Hogers		9 juni 2011
Email Security Issues status	L. van Riet	-	31 oktober 2011
Information Risk Rating Website	Information Security Forum	-	-
Thread Assessment Website	Information Security Forum	-	-
Vulnerability Assessment Website	Information Security Forum	-	-

Interviews en locale inspectie

Datum	Interview / lokale inspectie	Locatie	Perso(o)n(en)
20111103	Interview	EL&I	J. Majoor

App 3.6 Berichtenbox

Geraadpleegde documentatie

Document	Auteur	Versie	Datum
P127 Programma van eisen SURC Hosting	D. Mansvelder	-	-
Algemene voorwaarden SURC Hosting	-	-	31 mei 2006
Service Niveau Overeenkomst berichtenbox	J. Steenvoorden	1.0	3 november 2011
Offerte Anoigo	Anoigo	-	15 december 2010
Overeenkomst Anoigo	-	-	8 februari 2011
Dossie Afspraken en Procedures Berichtenbox	J. Steenvoorden	1.03	3 november 2011
Information Risk Rating Berichtenbox	Information Security Forum	-	-
Thread Assessment Berichtenbox	Information Security Forum	-	-
Vulnerability Assessment Berichtenbox	Information Security Forum	-	-
Functioneel ontwerp Berichtenbox, FO-01 – FO-22	A. Peree, K. Vels	…	11 oktober 2010
Handleidingen Berichtenbox H-04 – H-08	…	…	…
Koppelvlak specificaties KD-01 – KD-03 en KS-01	…	…	…
Non Functionele specificaties NF-1	K. Nieuwenhuys, K. Vels	1.1	2 november 2009

Technisch Ontwerp Berichtenbox, TO-1 en TO-2	…	…	…
Test documentatie Berichtenbox T-01, T-03, T-06 en T-07	…	…	…
Supplementary Speicifications Berichtenbox O-02	K. Nieuwenhuys,	1.0	20 december 2010
eOverheid voor Bedrijven Beveiligingsplan 2009	eOverheid voor Bedrijven	1.0	1 juli 2009
As Is Architectuur Berichtenbox	R. Hurkmans	1.0	14 augustus 2009

Interviews en locale inspectie

Datum	Interview / lokale inspectie	Locatie	Perso(o)n(en)
20111103	Interview	EL&I	P. Wolff
20111108	Interview		L. Ouwehand

App 4 VRAGENLIJST

De vragen vallen in 3 categorieën uiteen:

- Inleidende algemene vragen.
- Veiligheidsvragen, die op hun beurt onderverdeeld kunnen worden in:
  - Vragen met betrekking tot het ontwerp van de veiligheid (hoofdvraag A).
  - Vragen met betrekking tot de feitelijke werking van de veiligheid (hoofdvraag B).
- Dienstspecifieke veiligheidsvragen.

App 4.1 Inleidende algemene vragen

Nummer	Vraag	Bron
1.	Elke dienst kent minimaal de volgende rollen; eigenaar, toezichthouder, beheerder. Waar en door wie zijn deze ingevuld?	
2.	Welke rollen zijn er nog meer gedefinieerd en hoe en waar zijn deze ingevuld?	
3.	Wat zijn de consequenties van de wijze waarop rollen zijn gedefinieerd en belegd voor autorisaties?	
4.	Waar is het functioneel beheer van de dienst belegd?	
5.	Waar is het applicatie- en technisch beheer van de dienst belegd?	
6.	Hoe heeft u incident-, configuratie- en wijzigingbeheer ingericht? Zowel organisatorisch als procedureel.	
7.	Wie is eindverantwoordelijk voor de informatiebeveiliging?	[VIR]
8.	Waar is informatiebeveiliging van de dienst belegd?	
9.	Onder welke Wbp klasse valt de dienst? Tot welke maatregelen heeft dit geleid?	[Wbp]

App 4.2 Veiligheidsvragen

Nummer	Vraag	Bron
	Ontwerp veiligheid van de dienst	
10.	Heeft u in kaart gebracht welke wet en regelgeving voor u van toepassing is?	
11.	Is er een risicoanalyse gemaakt en actueel gehouden?	[VIR]
12.	Welke maatregelen zijn er in het ontwerp van de diensten ontworpen om de veiligheid te borgen?	
13.	Hoe wordt zekergesteld dat er voldoende aandacht is voor het dichten van achterdeuren bij het ontwerp, het afhandelen van incidenten en wijzigingsverzoeken?	
14.	Welke maatregelen zijn er voor de beheerfase van de diensten ontworpen om de veiligheid te borgen?	
15.	Hoe wordt zekergesteld dat er voldoende aandacht is voor het voorkomen van het ontstaan van achterdeuren door opzettelijke of onopzettelijke fouten van beheerders?	

Nummer	Vraag	Bron
16.	Is er een aparte omgeving voor ontwikkeling, test, acceptatie en productie?	
17.	Zijn de beveiligingseisen voldoende afgestemd met de dienstenleverancier van het platform waarop de dienst draait?	
18.	Is het toegangsbeleid vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen?	[ISO27002], paragraaf 11.1.1 [NORA]: paragraaf AP40
19.	Zijn er formele procedures vastgesteld voor het registreren/afmelden van gebruikers/beheerders en het verlenen/intrekken van toegangsrechten tot de dienst?	[ISO27002], paragrafen 11.2.1, 11.6.1 [NORA]: paragraaf AP37
20.	Wordt het gebruik van voldoende sterke en unieke authenticatiemiddelen of wachtwoorden afgedwongen?	[ISO27002]: paragrafen 11.2.3, 11.2.4, 11.3.1, 11.4.2, 11.5.2, 11.5.3 [1)] [NORA]: paragraaf AP37
21.	Hoe is zeker gesteld dat de dienst geen ongewenste interactie heeft met andere diensten?	[ISO27002], paragraaf 11.6.2 [NORA]: paragraaf AP38
22.	Worden gebruikers en beheerders na verloop van tijd automatisch van de sessie afgemeld?	[ISO27002], paragraaf 11.5.5 [1)] [NORA]: paragraaf AP37
23.	Op welk STORK niveau is authenticatie tot het verkrijgen van de dienst uitgevoerd en is het gekozen voldoende voor de dienst?	[STORKQAS],
24.	Welke beveiligingsoplossingen heeft u ontworpen? Met name: authenticatie, onweerlegbaarheid en opslag van gegevens en welke cryptografische technieken daarbij zijn gebruikt.	[NORA]: paragraaf AP40 [NORA]: paragraaf
25.	Welke vercijferingscertificaten zijn gekozen (bij de communicatie tussen platformen, beveiligde verbindingen)	
26.	Worden alle informatiebeveiligingincidenten tijdens de opzet gerapporteerd, beoordeeld en vertaald naar maatregelen?	[ISO27002], paragrafen 13.1 en 13.2
	Feitelijke werking veiligheid van de dienst	
27.	Zijn alle ontworpen maatregelen in het ontwerp van de dienst geëffectueerd?	
28.	Zijn alle ontworpen maatregelen voor de beheersfase van de dienst geëffectueerd?	
29.	Is de effectuering van de beveiligingseisen bij de dienstenleverancier van het platform waarop de dienst draait voldoende geborgd?	
30.	Zijn de procedures voor het registreren/afmelden van gebruikers/beheerders en het verlenen/intrekken van toegangsrechten tot de dienst voldoende geborgd?	[ISO27002], paragrafen 11.2.1, 11.6.1 [NORA]: paragraaf AP37
31.	Wordt de dienst regelmatig geaudit?	[ISO27002], paragraaf 15.2.2
32.	Wanneer is de dienst de laatste keer geaudit?	[ISO27002], paragraaf 15.2.2
33.	Wordt op de dienst regelmatig een penetratietest uitgevoerd?	[ISO27002], paragraaf 15.2.2

Nummer	Vraag	Bron
34.	Wanneer is op de dienst de laatste keer de penetratietest uitgevoerd?	[ISO27002], paragraaf 15.2.2
35.	Worden alle informatiebeveiligingincidenten gerapporteerd, beoordeeld en vertaald naar maatregelen?	[ISO27002], paragrafen 13.1 en 13.2
36.	Wordt het naleven van de procedures afgedwongen?	[ISO27002], paragrafen 15.2.1, 8.2.1 en 8.2.3

1) in paragraaf 11.5 wordt voor “besturingssystemen” “dienst” gelezen.