Auditdienst Rijk
Ministerie van Financiën

Quick scan informatiebeveiliging AGS- Bevindingen

Colofon

Titel	Quick scan informatiebeveiliging AGS - bevindingen
Uitgebracht aan	Belastingdienst Douane NL
Datum	19 oktober 2015
Kenmerk	ADR/2015/1396

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Inleiding

In de loop van 2015 is het systeem AGS voor het proces 'invoer', uitgezonderd de periodieke aangifte, volledig in gebruik genomen. Hierbij wordt voor tarieven- en maatregelenselectie gebruik gemaakt van het, ook nieuwe systeem, DTV. In eerdere ADR onderzoeken tijdens de projectfase van AGS is informatiebeveiliging van AGS wel deels aan de orde is geweest, maar een breed inzicht over de informatiebeveiliging van AGS ontbreekt nog.

Om meer inzicht te verkrijgen heeft de opdrachtgever de ADR verzocht om, via een quick scan, te inventariseren of, en op welke onderdelen, risico's worden gelopen op het gebied van informatiebeveiliging met betrekking tot (het gebruik van) het in productie genomen deel van de applicatie AGS. Daarbij is verzocht om specifiek na te gaan of voor langdurige uitval van AGS een uitwijkscenario is ingeregeld. Hieronder zijn ook DTV en het onderliggende infrastructurele platform, Business Process Hosting (BPH), begrepen.

Uit deze inventarisatie blijkt dat er nog diverse tekortkomingen zijn die een risico in zich houden dat het vereiste niveau van betrouwbaarheid[1] niet optimaal gegarandeerd is, dan wel niet volledig gerealiseerd zal worden.

1 Betrouwbaarheid omvat beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.

1 Niet inzichtelijk of de vereiste betrouwbaarheidsniveaus zijn afgedekt

Het risico bestaat dat het stelsel van eisen/voorgenomen maatregelen niet voldoende is voor de vereiste betrouwbaarheidsniveaus.

1.1 Volledigheid opgestelde eisen en maatregelen niet controleerbaar door ontbreken risicoanalyses

AGS en DTV zijn via aanbestedingstrajecten in 2008 en 2009 aangeschaft bij IBM. Daarbij zijn in de bestekken eisen zijn meegegeven. Aan die eisen liggen geen controleerbaar uitgevoerde risicoanalyses ten grondslag. De eisen in de bestekken zijn daarmee niet, via een dreigingenanalyse, navolgbaar afgeleid van een in een risicoanalyse vastgesteld betrouwbaarheids*niveau*.

1.2 Gering risico dat eisen, voor zover gesteld, niet zijn ingevuld

1.2.1 *Leverancier moet AGS en DTV leveren conform de eisen uit de bestekken*

De aanbestedingen konden alleen gegund worden als de leverancier aan alle gestelde eisen invulling gaf. Ons is medegedeeld dat de geselecteerde leverancier had aangegeven dat hij alle eisen had ingevuld.

1.2.2 *Via 'GAP workshops' vastgesteld dat opgeleverd product AGS voldoet aan de gestelde eisen*

Ons is meegedeeld dat voor AGS, middels zogenaamde 'GAP-workshops', is vastgesteld dat alle functionele eisen en wensen in het bestek voor zover ze nog relevant waren, zijn geleverd door de leverancier IBM. Een deel van de functionele eisen heeft betrekking op informatiebeveiligingsaspecten. Een vastlegging van deze workshops kon niet worden achterhaald.
Of dit ook voor DTV is gedaan is ons niet bekend.

1.2.3 *Controleerbare vaststelling dat eisen zijn ingevuld in opgeleverde producten ontbreekt deels*

- *Uitvoering van architectuurcontrol wordt niet formeel vastgelegd.*
  De eisen uit het bestek zijn, naar ons is medegedeeld, doorvertaald in de ICTSA's. Het bewaken dat die eisen vervolgens worden geïmplementeerd behoort tot de 'architectuurcontrol'. Een geïnterviewde architect geeft aan dat dit wel wordt uitgevoerd, maar daarvan geen formele vastlegging plaatsvindt.

- *Geen specifieke beveiligingsparagrafen in ontwerp- en fasedocumenten.*
  In relevante documenten (bestek, ICTSA, etc.) zitten de beveiligingseisen, voor zover aanwezig, verweven door het geheel. Er zijn geen specifieke beveiligingsparagrafen waarin aangegeven wordt wat de beveiligingseisen zijn en hoe ze zijn geïmplementeerd. Hierdoor is de navolgbaarheid van ontwerp naar implementatie betreffende de informatiebeveiliging beperkt.

- *Systeembeveiliging is deels getest.*
  - Er zijn geen specifieke systeembeveiligingstesten waarmee vastgesteld kan worden dat AGS aan de beveiligingseisen voldoet, op AGS uitgevoerd.
  - Via het VTA testtraject wordt wel functionaliteit getest, dus waar beveiligingseisen zijn ingevuld via functionaliteit is aannemelijk dat dit, risicogebaseerd, in de testen is meegenomen.
  - Er zijn wel specifieke Attack en Penetration testen op DTV uitgevoerd. Dit omdat DTV via internet een directe verbinding met de buitenwereld heeft.

2 Vereiste beschikbaarheid AGS en DTV onvoldoende gewaarborgd

Het risico bestaat dat het proces Aangiftebehandeling niet overeenkomstig de gestelde eisen beschikbaar zal zijn.

2.1 Voor AGS en DTV is de eis dat deze hoogbeschikbaar zijn

Aan AGS is in het bestek de eis gesteld van 99,5% beschikbaarheid. Naar ons is meegedeeld is dit recent verlaagd naar 98,5% omdat 99,5 % niet haalbaar is gebleken. Aangezien AGS zonder DTV niet kan werken, geldt die eis ook voor DTV en betekent dit ook dat het BPH platform hoogbeschikbaar moet zijn.

2.2 Hoogbeschikbaarheidsmaatregelen nog niet volledig ingevuld

2.2.1 *Het onderliggende platform, BPH, is (nog) niet hoog beschikbaar*

B/CIE heeft met betrekking tot DTV beschreven welke issues in het onderliggende infrastructurele platform maken dat DTV nog niet hoogbeschikbaar is. Deze gelden grotendeels ook voor AGS. De genoemde problemen kunnen deels pas worden opgelost nadat BPH is overgegaan van het platform AIX naar IPAS. Douane geeft aan dat een overgang naar IPAS niet zeker is, het kan ook BPM 8 worden. Dat is nog in onderzoek.

2.2.2 *Voorziene monitoring nog niet ingericht voor AGS en DTV*

De voorziene service monitoring, om productieverstoringen te signaleren en zo mogelijk te voorkomen, is nog niet ingericht. Aan B/CIE is de opdracht gegeven om de logfiles van AGS en DTV daarvoor gereed te maken. Ook de voorziene business event monitoring AGS is niet in de eerste release van AGS3 opgenomen. Dit blijkt uit de ICT Startarchitectuur (ICTSA) voor AGS3.

2.2.3 *Geen formele 7*24 stand-by regeling B/CAO*

Met IBM is afgesproken dat prio-1 verstoringen altijd binnen 4 uur opgelost zijn. B/CAO heeft echter, naar ons is medegedeeld, geen 7*24 uur stand-by formeel geregeld, waardoor het risico bestaat dat een door IBM bijtijds aangeleverde oplossing een tijdje blijft liggen voordat deze door B/CAO wordt opgepakt.

2.3 Geen uitwijkscenario aangetroffen

Een uitwijkscenario/-plan voor AGS en DTV, waarin aangegeven wanneer eventueel moet worden uitgeweken en wat daartoe moet worden gedaan, hebben wij niet aangetroffen. Aangegeven is dat CAO CIE heeft verzocht de status van een overall-calamiteitenplan uit te zoeken en dat daarbij wordt onderzocht in hoeverre dat plan een specifiek plan DTV-AGS overbodig maakt.

2.4 Performance van de keten onzekere factor

2.4.1 *Risico op daling performance AGS2 bij invoering AGS3*

Het is nog niet duidelijk hoe goed de gehele applicatieketen presteert. Het project AGS moet met IBM en B/CIE vaststellen in hoeverre de technische infrastructuur voor AGS opgeschaald moet worden. Ook voor KIS, PRISMA en DOBRA moeten performance-onderzoeken uitgevoerd worden om vast te stellen welke maatregelen er genomen moeten worden om de gevraagde performance te behalen. Bovenstaande is beschreven in de ICTSA voor AGS3.
In de afstemming van het conceptrapport geeft Douane aan dat de performance testen in de fabriek van IBM zijn uitgevoerd en dat de performance testen in de

keten in de maanden september en oktober worden uitgevoerd. Zij geeft daarbij aan dat uit de testen blijkt dat de gevraagde performance wordt gehaald.

2.4.2 *Vollopen databases DTV kan performance nadelig beïnvloeden*

Ons is aangeven dat het risico bestaat dat de performance van DTV nadelig wordt beïnvloed doordat databases (incl. logs) van DTV aan het vollopen zijn. Er is en wordt gewerkt aan schoning van de databases. Douane geeft hierbij aan dat het hier gaat om technische logs en niet om functionele logs.

3 Enkele te ruim verstrekte rechten

Het risico bestaat dat bewust of onbewust:

- *aangiftegegevens van aangiften die al zijn afgehandeld ten onrechte gewijzigd worden waardoor aangiftegegevens niet meer aansluiten op het heffingsbedrag;*
- *aangiften ten onrechte op 'handmatig afdoen' worden gezet en daardoor vertraging oplopen in de verwerking.*

3.1 AGS autorisatierol 'modify declaration' te ruim uitgegeven

De rol 'Modify declaration' die het mogelijk maakt *reeds afgehandelde* aangiften te wijzigen is verstrekt aan 253 medewerkers van Douane (stand 01-07-2015). Deze rol is echter bestemd voor beheer (B/CA).

In de afstemming van het conceptrapport heeft Douane aangegeven dat de betreffende autorisaties inmiddels zijn ingetrokken.

3.2 Nationale Helpdesk Douane te ruime rechten voor AGS

De beheerder B/CA geeft aan dat de Nationale Helpdesk Douane dezelfde autorisaties met betrekking tot AGS heeft als de groep van 4 AGS beheerders van B/CA en dat de helpdesk daarmee te ruime rechten heeft in het systeem

De beheerautorisatie houdt o.a. in dat berichten handmatig afgedaan kunnen worden. Als er iets is vastgelopen, kan een beheerder het bericht er uithalen en dan doorgeven aan Douane, die het buiten het systeem verder afhandelt. De helpdesk hoeft dit niet te kunnen doen volgens de beheerder. Wel zou de helpdesk berichten moeten kunnen herverzenden.

4 Diverse punten nog niet optimaal ingericht

Het risico bestaat dat:

- *verstoringen niet tijdig worden opgemerkt waardoor de gerealiseerde beschikbaarheid kan dalen;*
- *een niet juist of volledig transmissiebestand verwerkt wordt, waardoor fouten in de tarieven en maatregelen, en daardoor in de heffing, ontstaan;*
- *Business rules van AGS fouten bevatten die niet (tijdig) worden opgemerkt waardoor de integriteit van de verwerking wordt geschaad;*
- *het beheer door B/CA UDO niet optimaal kan worden uitgevoerd waardoor de betrouwbaarheid van de verwerking kan worden geschaad*;
- *bewuste of onbewuste fouten in handmatige behandelingen van aangiften niet worden voorkomen of ontdekt met mogelijke gevolgen voor de juistheid en volledigheid van de heffing en de tijdigheid van de afhandeling.*

4.1 Logging nog niet naar wens ingericht en niet pro-actief benut

4.1.1 *DTV auditlogging nog niet (volledig) gerealiseerd*

In de ICTSA DTV release 2015-2 is vermeld dat de volgende eisen nog niet (volledig) zijn gerealiseerd.

- Eis FUN.25: 'Het Tariefsysteem moet een logging systeem hebben, waarmee herleidbaarheid van handelen te realiseren is. De beveiligingslogbestanden moeten toegankelijk zijn voor analysetools. De integriteit van opgeslagen logbestanden moet gewaarborgd zijn, en logbestanden moeten niet achteraf aangepast kunnen worden.'
- Eis FUN 26: 'De bewaarduur van de loginformatie moet instelbaar zijn. De bewaarduur betreft het aantal dagen dat loginformatie bewaard moet blijven na het moment dat deze informatie in de log geschreven is.'

4.1.2 *Geen pro-actief gebruik van logbestanden*

AGS en DTV hebben diverse loggingen. Deze worden vooral re-actief (bij incidenten en problemen) gebruikt. De logging wordt niet pro-actief gebruikt ten einde beveiligingsincidenten of de juiste werking van het systeem vast te stellen.

4.2 Enkele belangrijke bestanden niet voorzien van efficiënte controlevoorziening

4.2.1 *De (DTV) transmissiefiles zijn niet voorzien van hashtotalen*

Transmissiefiles waarmee de tarief- en maatregelmutaties vanuit DG Taxud worden aangeleverd hebben geen voorziening, bijvoorbeeld hashtotaal, waarmee kan worden vastgesteld dat ze tijdens transport niet gewijzigd zijn. Ze hebben wel een volgnummer, zodat de volgorde van verwerken kan worden bewaakt. DTV controleert de berichten wel op het juiste formaat. De architect DTV van B/CAO geeft aan dat m.b.t. het berichtenverkeer over het CCN netwerk is besloten dat er geen extra beveiligingsmaatregelen nodig zijn omdat het CCN netwerk goed beveiligd wordt geacht. O.i. bestaat er een gering risico dat de bestanden beschadigd worden en dat dit niet wordt opgemerkt.

4.2.2 *Controle Business rules AGS als geheel niet goed mogelijk doordat niet voorzien is in een controlevoorziening*

Het wijzigingenproces van business rules is een proces tussen Douane IM en B/CA UDO (beheer). Douane IM noch B/CA controleert (periodiek) of alle business rules nog zijn zoals ze moeten zijn. Er is niet voorzien in een controlegetal of iets dergelijks waarmee dat efficiënte kan worden uitgevoerd. Wel controleert IM bij mutaties of deze goed zijn doorgevoerd.

AGS bewaart de historie van business rules. Dit is noodzakelijk omdat oude regels nog gelden voor oude aangiftes. Van *verwijderde* business rules is echter geen historie meer beschikbaar; ze zijn geheel weg uit AGS.

4.3 Aanbevolen rapportages voor controledoeleinden niet te realiseren

In 2012 heeft de ADR aanbevolen[2] om voor controledoeleinden rapportages of andere faciliteiten te ontwikkelen op basis waarvan:

- de handmatig uitgevoerde berekeningen en
- het ongeldig maken van aangiften, of, breder, het handmatig innemen van een Douanestandpunt

kunnen worden gecontroleerd cq. geautoriseerd.
In deze quick scan is ons aangegeven dat dit nog niet gerealiseerd is.

In de afstemming van het conceptrapport geeft Douane aan dat de taak 'handmatig uitgevoerde berekeningen' een risicoclassificatie is gekoppeld waardoor deze taak aan een beperkt aantal medewerkers kan worden toegekend. Ten aanzien van de taak 'ongeldig maken' geeft Douane bij de afstemming aan dat hierop in de operatie een IC wordt uitgevoerd en dat in AGS 3 deze taak geïsoleerd is van andere taken, zodat ook deze taak aan een beperkt aantal medewerkers kan worden toebedeeld.

4.4 Beheer B/CA nog niet optimaal toegerust

B/CA UDO geeft aan dat diverse zaken, die zij nodig acht voor het goed uit kunnen voeren van het beheer betreffende DTV, nog niet of niet goed geregeld zijn. Dit betreft ondermeer:

- *Beheren en gebruiken van logbestanden;*
  DTV en AGS vullen meerdere logbestanden. DTV beheerders van B/CA geven aan dat deze logbestanden hen, voor raadpleging, ter beschikking moeten staan en dat het bij verstoringen noodzakelijk is deze te downloaden en te voegen bij de registratie van de verstoring. Zij geven hierbij aan dat momenteel beveiligingseisen niet gerealiseerd zijn vanwege toegangseisen tot logbestanden. Ook de architect AGS en DTV van B/CAO geeft aan dat het raadplegen van logbestanden verbeterd kan worden.

- *Beheren transmissiefile tarieven en maatregelen*;
  Tarieven en maatregelen in DTV worden elke werkdag bijgewerkt vanuit een door DG Taxud aangeleverde transmissiefile. Als er een fout zit in de transmissiefile die niet binnen de applicatie DTV kan worden opgelost is het noodzakelijk de transmissiefile van het systeem te halen. Hiertoe zijn volgens B/CA rechten nodig op verschillende mappen.

- *Onvoldoende kennis over applicaties t.b.v. beheer SIbus en FEM*
  Door ontbrekende informatie en documentatie over beheerapplicaties SIbus[3] en FEM (Failed Event Manager) is daar volgens B/CA onvoldoende kennis over. Bij het beheer van AGS hebben wij geconstateerd dat in FEM meldingen staan waarvan de beheerder niet weet wat ze betekenen en wat er mee te doen. O.i. bestaat het risico dat deze fout-events ten onrechte niet worden hersteld.

- *Monitoringmogelijkheden MQ*;
  DTV maakt (voor koppelvlakken) gebruik van diverse message queues (MQ) op het mainframe. B/CA geeft aan dat het voor het beheer mogelijk moet zijn om de MQ's te kunnen monitoren om tijdig in te kunnen grijpen.

2 Aanbeveling H3 uit rapport ADR/2012/1082
3 Een beheertool bij Webshere Application Server; service integration bus van IBM

- *Beperkingen op zoekmogelijkheden DTV;*
  B/CA beheerders geven aan dat zij op dit moment de volledigheid van uitgaande en ontvangen berichten en de juiste werking van DTV niet kunnen vaststellen. Zoekmogelijkheden, ook in Statistics en Quota en queries, zijn beperkt.

Bovenstaande punten zijn al onderwerp van gesprek tussen Douane (IM), B/CAO, B/CIE en B/CA.

5 Beveiligingsrisico's in platform BPH

De informatie op deze pagina is in het belang van de veiligheid van de Staat

6 Ondertekening

Utrecht, 19 oktober 2015

Projectleider ADR

Bijlage 1; Plan van aanpak inclusief toelichting onderzoek

Bijlage 1 bestaat uit het plan van aanpak waaraan in paragraaf 2.1.1 blokken tekst in kaders zijn toegevoegd waarin voor de onderzoeksvragen aangegeven wordt hoe of waar deze in het rapport zijn beantwoord.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00