januari is daarnaast het memo 'Waarborgen integriteit bij W&S' besproken. Het DTBD heeft de behoefte uitgesproken om het risico op ongewenste infiltratie via het wervingsproces te minimaliseren en heeft verzocht om een verscherpt kader op integriteitsscreening aan de voorkant van het instroomproces. De adviezen vanuit de Douane geven richting aan deze vraag.

Het DT BD geeft brede steun voor de versterking op screening. En geeft aan P-gv. mee om oog te hebben voor de privacy aspecten (irt AVG), medezeggenschap aspecten en de financiële gevolgen vanwege extra inzet (deze worden opgelost binnen bestaande kaders). P-gv. wil graag in gesprek treden over de aanpak en ervaringen delen.

Besluit:
Het DT BD gaat akkoord met de volgende beslispunten:
- het DT BD ondersteunt de richting van het MT Douane.
- het DT BD stemt in met het onderzoeken welke maatregelen Belastingdienst breed in dezelfde lijn toegepast kunnen worden (langs de weg van bespreking in het driehoeksoverleg O&P).
- het DT BD ondersteunt de uitvoering van de pilot.
- het DT BD stemt in met het opstellen van een zwarte lijst.
- het DT BD stemt het DTBD in met een tijdelijke ontheffing van de beleidsbeperking in de PUB.
- het DT BD stemt in met screening van Belastingdienstmedewerkers die doorstromen naar de Douane.
- De uitwerking zal in de vorm van concrete acties zal worden opgepakt. E.e.a. komt terug in de driehoek O&P. Dit zal resulteren in een Kamerbrief vóór de zomer. =>ACTIE Persoonsgegevens
- In de driehoek O&P zal ook besproken worden welke andere risicovolle functies er binnen overige BD-onderdelen zijn waarvoor versterking van screening nodig wordt geacht. =>ACTIE Persoonsgegevens
- P-gv. verzoekt om waar nodig formele verzoeken per brief aan derden te stellen en dit via P-gv. te laten lopen ten behoeve van een ordentelijk bestuurlijk proces en uit het oogpunt van integriteit.

B3. Doelstelling Wet Banenafspraak
Ingebracht door P-gv..

Conform afspraak in het DT BD van 25 april 2019 ligt een aangepaste aanpak voor, ter realisering van de banenafspraak.
P-gv. benadrukt dat er voor 2019 nog een forse inspanning nodig is van iedereen. De randvoorwaarden, te weten een goede projectorganisatie en budget, liggen nu ter besluitvorming voor.
DT BD geeft brede steun aan de voorliggende aanpak en geeft daarbij mee om de onderlinge samenwerking op dit onderwerp te verbeteren, lokaal de verbinding te houden en vooral het werk te zoeken bij de mensen (i.p.v. de reguliere werkwijze andersom).

Besluit:
Het DT BD stemt in met:
- het vrijstellen van een groep ervaren medewerkers om arbeidsparticipanten te werven en plaatsen bij onderdelen van de BD;
- indien nodig 1 participant per team te realiseren;

- het minimaliseren van beperkingen t.b.v. realisatie van de doelstelling.
- Afgesproken wordt om regelmatig een update te geven in het DT BD, als eerste vóór de zomer, en vervolgens direct na de zomer **=>ACTIE** Persoonsgegevens

B.4 Budgettoekenning programma "Maak het mogelijk!"
Ingebracht door P-gv., vertegenwoordigd door P-gv..

Besluit:
Het DT BD besluit, in navolging op de besluitvorming bij punt B3:
1) akkoord te gaan met meerjarig (2019 t/m 2023) formatie, inhuur- en materieel budget voor het programmateam.
2) akkoord te gaan met meerjarig (2019 t/m 2023) formatie, inhuur- en materieel budget voor de job coaches.
3) om meerjarig (2019 t/m 2023) materieel budget toe te kennen voor het centrale team Schoonmaak. De werkwijze m.b.t. centrale team P-Direkt blijft ongewijzigd.

B.5 Bijzonder belonen teamuitjes
Het gehele agendapunt en de besluitvorming daarover vervalt. Dit is conform de overlegvergadering van 29 mei jl. met de COR, waarin het besluit teamuitjes is ingetrokken.

B.6 Toekenning VJN middelen
Ingebracht door P-gv..

Bij voorjaarsnota zijn middelen toegekend voor ondermijning, witwassen en toezicht. Er zijn minder middelen toegekend dan origineel aangevraagd. Dit leidt er toe dat keuzes gemaakt moeten worden in de verdeling.
P-gv. koppelt de in de driehoek C&F in deze gemaakte afspraken terug. Namelijk, de opbouw van de middelen reeksen is reeds aangepast; verder zijn de huisvestingskosten verrekend en zijn de FTE's gekoppeld aan de primaire trekkers (dit speelt bijvoorbeeld bij CAP). Teruggekeken wordt op een succesvol traject.

Besluit:
Het DT BD stemt in met het voorstel om de voorliggende verdeling van de middelen voor de claims ondermijning, witwassen en toezicht uit te werken voor de Bestuursraad. Met de volgende afspraken:
-dat via uitvoeringstoetsen keuzes worden voorgelegd en waar nodig belangrijke besluiten op de juiste tafels (bijvoorbeeld bij de Staatssecretaris) ter sprake worden gebracht; indien er verzoeken komen vanuit het Europees OM, dan zal dit ten koste gaan van de nationale capaciteit die de FIOD kan inzetten.
-dat de tekst bij ondermijning wordt aangepast (het gaat niet alleen aanpak van ondermijnende criminaliteit voor organisaties van J&V in de strafrechtketen).
-het DT BD vraagt in aanvulling aandacht voor de wijze van verantwoorden; hoe kunnen de baten zowel kwalitatief als kwantitatief in beeld worden gebracht (gelet op de leerervaringen ITI), **=>ACTIE** P-gv. **en** P-gv. **werken dit uit.**

Er wordt een notitie voor de staatssecretaris voorbereid hoe de middelen ingezet zullen gaan worden, **=>ACTIE** Persoonsgegevens

B.7 Eerste viermaandsrapportage Belastingdienst 2019
Ingebracht door P-gv. .

In de 4MR wordt gerapporteerd over de voortgang op de uitvoering van het Jaarplan Belastingdienst. De opzet en structuur van de 4MR is gebaseerd op de aanschrijving van P-gv. .
De 4MR schetst het beeld dat de BD grote inspanningen verricht maar er nog een lange weg te gaan is.

Besluit:
Het DT BD stemt in met het nu voorliggende concept van de 1e 4MR BD 2019.
Met de aanpassingen:
-dat in de VMR en reflectie prominenter wordt ingegaan – in aansluiting op de conclusies in het traject Stapeling – op de voorziene afname van de financiële kaders waarmee de uitvoering van taken en van de vernieuwingsopgave onder druk komt. Met daarbij de toezegging dat momenteel verdere verdieping van de problematiek plaatsvindt en in de tweede VMR concreet geduid zal worden welke problemen voorzien worden en waarop moet worden bijgestuurd. Zodat hierover vroegtijdig het gesprek met P-gv. gevoerd kan worden.
-het DT BD constateert dat de beschreven risico's vooral risico's die terugblikken zijn. DT-leden heroverwegen deze opgenomen risico's vanuit deze optiek,
=>ACTIE ALLEN.

C STUKKEN TER BESPREKING

C.1 Innovatievisie
Dit punt wordt doorgeschoven naar DT 6 juni.

C.2.a AVG, voortgang t/m april 2019 en C.2.b stand van zaken applicaties, schonen en vernietigen persoonsgegevens
Ingebracht door P-gv.

Het agendapunt AVG gaat over de voortgang van de uitvoering van de maatregelen AVG met als uiterlijke einddatum 25 mei 2019. Bijgevoegd is een bijlage met de nog openstaande maatregelen van de bedrijfsonderdelen. Daarnaast is bijgevoegd de notitie over stand van zaken van de applicaties aangaande het schonen en vernietigen van persoonsgegevens.

Het DT BD concludeert:
-er is grote vooruitgang geboekt en de directies zijn in control, met uitzondering van het schonen van de verouderde gegevens. Ook wat betreft het op orde brengen van de systemen zonder eigenaar is progressie zichtbaar. Er is wel blijvende aandacht nodig.
-in de Kamerbrief die in voorbereiding is, zal gemeld worden dat de AVG geen statisch gegeven is, maar een proces dat voortdurend aandacht vergt.
-aan de ADR zal gevraagd worden om een update te doen of de aanbevelingen goed verwerkt zijn. P-gv. vraagt of dit z.s.m. in gang kan worden gezet, zodat de resultaten kunnen worden opgenomen in de eerstvolgende rapportage aan de Kamer.

P-gv. zal in de VMR-gesprekken vragen naar een plan van aanpak 'opschoning'. Hierin wordt ingegaan op welke wijze de opschoning gerealiseerd kan worden (om

hoeveel oude documenten het gaat en hoeveel opschoningstijd er mee gemoeid is), ***=>ACTIE alle primair procesdirecteuren.***

P-gv. geeft aan dat volgende maand wederom een zelfde rapportage komt, daarna zal worden overgegaan op een tweemaandelijkse rapportage.

C.3 Bijdrage BD voor ontwerpbegroting IX 2020

Ingebracht door P-gv. en P-gv.

Op 25 april zijn de contouren van begroting IX 2020 besproken in het DT BD en op 16 mei is de bijdrage voor begroting IX 2020 besproken in de Concernstaf. Het DT BD wordt met dit memo meegenomen in de nadere uitwerking van de begroting en om zijn mening gevraagd over het 1e concept van de beleidsagenda en de begrotingsartikelen.

P-gv. geeft aan dat het proces nog gaande is, onder meer wordt de beleidsagenda getoetst.

Besluit:
Het DT BD is akkoord met de nadere uitwerking.

C.4 Projectenrapportage Vernieuwingsrapportage en Grote Projecten t/m april 2019

Ingebracht door P-gv..

Het DT BD concludeert:

- P-gv. doet de oproep aan allen om extra aandacht te geven aan de vijf beheerst vernieuwingsprojecten, die nu op rood/oranje staan, en te escaleren richting P-gv. indien nodig; en voorts de stamgegevens en mijlpalen goed in te vullen.
- Daar waar sprake is van vertraging wordt DT-leden gevraagd concreter aan te geven wat de oorzaken zijn van de vertragingen, zodat ook beter gestuurd kan worden.
- P-gv., P-gv. en P-gv. bezien en petit comité de gehanteerde definities rood / oranje / groen.

D STUKKEN TER KENNISNEMING

D.3 Bestuurlijke notitie voortgang vernieuwingsprojecten

Ingebracht door P-gv.

Dit betreft de bestuurlijke notitie over de voortgang van de vernieuwing. Deze notities worden maandelijks opgesteld voor de bewindspersonen. Ter informatie wordt de notitie t/m maart aan het DT aangeboden.
De minister en de staatssecretaris hebben geen vragen of opmerkingen bij deze notitie geplaatst. De bestuurlijke notitie wordt 27 mei besproken met de staatssecretaris tijdens het werkoverleg.

D.4 Moties en Toezeggingen

D.5 Periodiek overzicht door DG geaccordeerde dossiers 1-14 mei 2019

D.6 Overzicht vastgestelde uitvoeringstoetsen 2019

D.7 Verslagen Driehoeksoverleggen en ketentafels

D.8 Afronding Project noodvoorziening RAM
Ingebracht door P-gv..

De voorziening RAM voldeed niet aan vereisten vanuit het perspectief van informatiebeveiliging (AVG) en daarnaast waren er aandachtspunten vanuit het kunnen borgen van de continuïteit (techniek). In 2018 is besloten deze voorziening versneld te vervangen waarbij in eerste instantie een tijdelijke voorziening is neergezet om de continuïteit voor de business te kunnen borgen en vervolgens het MVP voor de toekomst vaste voorziening is neergezet. Dit project is afgerond. Dit betekent dat:
1. Het intrekken van de autorisaties op de Oracle database wordt op 24-5-2019 geeffectueerd. Het uitfaseren start op 25-5-2019 en volgt daarmee meteen op het intrekken van de autorisaties, waarbij de laatste actiepunten t.a.v. de uitfasering zijn belegd bij GBS.
2. MKB implementeert uiterlijk 24-5-2019 een specifiek omschreven AO/IC ten behoeve van het in gebruik nemen van de tijdelijke spoor 2 voorziening en neemt verantwoordelijkheid vanaf 2-5-2019 t.a.v. het in gebruik nemen van deze tijdelijke voorziening door geautoriseerde medewerkers.

D.9 Concept verslag COR 18 april 2019

E HAMERSTUKKEN
E.1 Procesbeschrijving teamuitjes
Het gehele agendapunt en de besluitvorming daarover vervalt. Dit is conform de overlegvergadering van 29 mei jl. met de COR, waarin het besluit teamuitjes is ingetrokken.

E.2 Projectplan herijking KPI's Belastingdienst
Ingebracht door P-gv., P-gv..

Het project heeft als opdracht een set strategische, effectgerichte indicatoren op te stellen. Deze set is gericht op artikel 1 van begroting IX voor 2021. Er zullen expertsessies worden gehouden met (vertegenwoordigers van) de uitvoeringsdirecties om de strategische doelstelling uit te werken naar activiteiten (doelenhiërarchie) en bijbehorende kpi's op te stellen. De uitvoeringsdirecties zijn hiervoor reeds benaderd.

Besluit:
Het DT BD stemt in met het projectplan voor de herijking van de KPI's. Dit projectplan is 12 april jl. behandeld in de driehoek C&F en 16 april goedgekeurd in de concernstaf.

E.3 Plan van aanpak verbeteren verplichtingenbeheer
Ingebracht door P-gv..

Met het plan van aanpak wordt invulling gegeven aan de aanpak van de onvolkomenheid die de Algemene Rekenkamer heeft geconstateerd op het verplichtingenbeheer bij de Belastingdienst. Het plan van aanpak bevat

aangescherpte kaders voor het verplichtingenbeheer en actiepunten om de sturing op de verplichtingen aan te passen.

Besluit:
Het DT BD stemt in met bijgevoegd plan van aanpak voor het verbeteren van het verplichtingenbeheer. In de toelichting van de nota zijn de acties en het tijdpad voor de budgethouders, SSO F&MI en C&F opgenomen.

F ALGEMEEN AFRONDEND

F.1 Rondvraag

P-gv. vertrekt, P-gv. neemt het voorzitterschap over bij het personeelsvertrouwelijke deel.

F.2 Personeelsvertrouwelijk

F.3 Afsluiting

Kerncijfers Handel in Auto 2018

Concept V6

Versie 6

Datum augustus 2018

Persoonsgegevens

Inhoud

Voorwoord 3

Managementsamenvatting 3

Doelgroep 3

A Indeling volgens branchecode 3

B Indeling aan de hand van transacties van voertuigen 4

C Aansluiting econ. branchecode met indeling Kamer van Koophandel 5

Conclusie samenstellen doelgroep 6

Telling op fiscaalnummer niveau 6

Telling op entiteitniveau 6

Samenloop HSB bestanden en branche indeling autohandel 7

Omzet voor de OB 2015-2017 8

Kasstroom 2015-2017 9

Invordering mei 2018 11

Juist en volledig 2016 en 2017 veldtoets 11

Risico indeling 13

Fiscaal dienstverlener 13

Externe informatie 15

Voorwoord

Ter ondersteuning van het project Auto (projectcode 2075) zijn een aantal kerncijfers verzameld die inzicht geven in omvang en fiscaal belang van de entiteiten die zich bezighouden met de handel in auto's. Doel van de dataverzameling is om de focus te verbreden, de zichtbaarheid van de Belastingdienst als toezichthouder te vergroten en de aanpak te differentiëren. Er zal een start gemaakt worden op de kantoren Groningen, Emmen, Leeuwarden, Enschede, Zwolle en Almere. De projectleider is Persoonsgegevens .

Er is gekozen om In deze rapportage aandacht te besteden aan de samenstelling van de groep autohandelaren en de omvang van de omzet en de kasstroom. Daarmee wordt duidelijk wie een belangrijke bijdrage doet in de staatskas maar ook welk belastingmiddel er toe doet. Ook wordt aandacht besteed aan de nalevingstekorten: er zijn inzichten in deze rapportage opgenomen van de invorderingsachterstand maar ook over de onjuistheid/onvolledigheid wordt gerapporteerd met behulp van de veldtoets gegevens uit IKB. Ook het "niet registreren" komt aan bod.

Managementsamenvatting

Nog maken

Doelgroep

Het bepalen van de doelgroep heeft plaatsgevonden op 2 manieren, namelijk via een subjectgerichte wijze (de ondernemer) en via een objectgerichte aanpak (de auto). Duidelijk is dat niet alle autohandelactiviteiten behandeld worden in aandachtsgebied Handel en Transport (H&TR). Vanwege de regels van entiteitopbouw kan de autohandelactiviteit ondergeschikt zijn binnen de entiteit en wordt de entiteit ingedeeld overeenkomstig de hoofdactiviteit. Uitgangspunt bij het bepalen van de groep autobedrijven is de branchecode indeling op fiscaalnummer niveau. Vervolgens zijn bij de betreffende fiscaal nummers de entiteitnummers gevoegd. De entiteiten die vallen onder MKB bestaan uit MKB, VIP en Convenantposten. MKB is te splitsen in MKB Midden en Kleine ondernemingen. De andere segmenten zijn GO, Buitenland, Stivers en Fictieve entiteiten.

A Indeling volgens branchecode

De branchecodes waarin veronderstelt wordt dat autohandel voor kan komen staan in tabel 1. Er zijn ook branches als autoverhuurbedrijven, leasebedrijven, taxibedrijven enz. waar veel auto's na gebruik verkocht worden. Deze blijven hier buiten beschouwing.

Tabel 1

Branche code	Brancheomschrijving	Doel groep nr	Doelgroepnaam	Segmentnr	Segment
6187	GROOTHANDEL IN AUTO'S EN AUTO-ACCESSO	05	AUTOHANDEL	51420	Dealerbedrijven
6387	TUSSENHANDEL IN AUTO'S EN AUTO-ACCESS	05	AUTOHANDEL	51420	Dealerbedrijven
6621	DETAILHANDEL IN NIEUWE PERSONENAUTO'S	05	AUTOHANDEL	51420	Dealerbedrijven
6623	DETAILHANDEL IN AUTO-ACCESSOIRES EN -	05	AUTOHANDEL	51420	Dealerbedrijven
6622	DETAILHANDEL IN GEBRUIKTE PERSONENAUT	05	AUTOHANDEL	51430	Gebruikte handel
6296	AUTOSLOPERIJEN	05	AUTOHANDEL	51570	Reparatiebedrijven
6496	AUTOSLOPERIJEN (TUSSENHANDEL)	05	AUTOHANDEL	51570	Reparatiebedrijven
6821	AUTOREPARATIEBEDRIJVEN (GARAGES) E.D.	05	AUTOHANDEL	51570	Reparatiebedrijven
6829	AUTOREPARATIEBEDRIJVEN, GESPECIALISEE	05	AUTOHANDEL	51570	Reparatiebedrijven

B Indeling aan de hand van transacties van voertuigen

Met behulp van het "Voertuigenbestand" in RAM, waarin 10,5 miljoen unieke finrs staan vermeld, is een selectie gemaakt van entiteiten die in de jaren 2015, 2016 én 2017 minimaal 10 auto's op naam hebben gehad, dan wel in een van die jaren minimaal 25 op naam hebben gehad (dat is het totaal van de transacties van sofinummers binnen een entiteit). Op deze wijze wordt via het object auto getoetst of het gebruik van bovenstaande branchecodes correct is. Starters en stakers komen op deze wijze in beeld, als ook bedrijven en particulieren die schommelen met verkopen boven en onder 10 auto's. Er zijn op deze wijze entiteiten 15.720 gedetecteerd. De doelgroepen waaraan deze entiteiten zijn toebedeeld staan hierna genoemd in tabel 2. Duidelijk is dat meer dan 2/3 valt onder doelgroep Autohandel. Opmerking: er is nog geen onderscheid gemaakt tussen de segmenten.

Tabel 2

Doelgroep	Aantal	Percentage
Leeg	264	1.68%
Autohandel	11.191	71.19%
Bouw	467	2.97%
Financiële dienstverl.	136	0.87%
Handel	1.148	7.3%
Horeca	103	0.66%
Industrie	258	1.64%
Landbouw & Visserij	86	0.55%
Medische dienstverl.	86	0.55%
Non-profits	144	0.92%
Persoonlijke dienstverl.	162	1.03%
Transport & Opslag	675	4.29%
Zakelijke dienstverl.	1.000	6.36%
Totaal	15.720	100%

De verdeling van de entiteiten uit het "Voertuigenbestand" over de branches is opgenomen in tabel 3. Ook hier is zichtbaar dat 2/3 van alle transacties plaatsvinden bij de vijf meest voor de hand liggende branchecodes. Omdat de focus ligt op autohandel dient detailhandel in motorfietsen buiten beschouwing te blijven.

Tabel 3

Br.code	Br.code omschrijving	Aantal	Percentage
6622	DETAILHANDEL IN GEBRUIKTE PERSONENAUTO'S	4.882	31%
6821	AUTOREPARATIEBEDRIJVEN (GARAGES) E.D.	3.206	20%
6621	DETAILHANDEL IN NIEUWE PERSONENAUTO'S	944	6%
6187	GROOTHANDEL IN AUTO'S EN AUTO-ACCESSOIRES (INCL. BANDEN)	797	5%
6387	TUSSENHANDEL IN AUTO'S EN AUTO-ACCESSOIRES EN ONDERDELEN (BANDEN)	400	3%
6625	DETAILHANDEL IN MOTORFIETSEN (INCL. ACCESSOIRES)	284	2%
Overige	Aantal overige branches 510	5.207	33%
Totaal		15.720	100%

In tabel 4 is de indeling van de entiteiten over de aandachtsgebieden en de segmenten weergegeven.

Tabel 4

Segment	LEEG	H&TR	KO	AR&D	VG&L	NVT	Totaal
MKB	0	7.114	6.001	552	342	0	14.009
CNV	0	374	80	81	29	0	564
VIP	0	16	11	7	0	0	34
GRO	0	0	0	0	0	840	840
FIC	0	0	0	0	0	13	13
STV	0	0	0	0	0	7	7
BTL	0	0	0	0	0	2	2
LEEG	251	0	0	0	0	0	251
Totals	251	7.504	6.092	640	371	862	15.720

De segmentindeling wordt als volgt als enkel de 5 meest relevante branchecodes uit tabel 3 worden geselecteerd. In totaal blijven er dan nog 10.229 entiteiten over waarvan 9.715 behoren tot de vermoedelijke doelgroep.

Tabel 5

Segment	H&TR	KO	NVT	Totaal
MKB	5.489	4.226	0	9.715
CNV	289	56	0	345
VIP	10	9	0	19
GRO	0	0	149	149
BTL	0	0	1	1
Totaal	5.788	4.291	150	10.229

C Aansluiting econ. branchecode met indeling Kamer van Koophandel

Om een oordeel te krijgen over de juistheid van de branchecode indeling is een vergelijk gemaakt met de indeling volgens de KvK. Zie onderstaande tabel 6.

SBICODE	OMSCHRIJVING	AANTAL
45112	HANDEL IN EN REPARATIE PERSONENAUTO'S EN LICHTE BEDRIJFSAUTO'S (GEEN IMPORT NIEUWE)	6184
45192	HANDEL IN EN REPARATIE ZWAARDERE BEDRIJFSAUTO'S (GEEN IMPORT NIEUWE)	288
45111	IMPORT NIEUWE PERSONENAUTO'S EN LICHTE BEDRIJFSAUTO'S	166
45191	IMPORT NIEUWE BEDRIJFSAUTO'S	23

In 76 % van de gevallen is het finr zowel met een branchecode als met een SBI code bekend als autohandelaar. In 4 % was er enkel een branchecode autohandel en in 8 % van de gevallen was sprake van enkel SBI code autohandel. In 12 % was er in het geheel geen sprake van autohandel. Er is geconstateerd dat in een aantal gevallen wel autohandel activiteiten plaatsvinden bij bijv. VOF, maar dat de registratie in het voertuigenbestand dan geregistreerd wordt via de vennoot.

Conclusie samenstellen doelgroep

Deze rapportage zal zich beperken tot de branchecodes 6621, 6622, 6187, 6387 en 6821, resp. handel in nieuwe auto's, tweedehands autohandel, garagebedrijven en groothandel -en tussenhandel in auto's en materialen. Dit zijn de branches waarin de meeste autohandel zich voordoet. De activiteit op finr niveau is daarbij bepalend. Bij het betreffende finr wordt de entiteit gevoegd. Dit wordt gecombineerd met de informatie over bedrijven die minimaal 10 auto's per jaar verhandelden in de jaren 2015 t/m 2017 dan wel in een van die jaren minimaal 25 auto's hebben verhandeld.

De rapportage richt zich op de bedrijven die zijn opgenomen in het segment MKB, dat zijn dus de 3 aandachtsgebieden in MKB Midden als ook aandachtsgebied MKB Klein.

Wijziging: tijdens de eerste bespreking met de leden van de projectgroep op 6 september 2018 is besloten om de ondergrens van de verkochte auto's te verhogen naar minimaal 25 in een van de jaren 2015, 2016 of 2017. De rapportage zal zich verder richten op de genoemde pilotkantoren.

Telling op fiscaalnummer niveau

Op basis van de 5 branchecodes zijn 36. 671 finrs geselecteerd, waarbij er in zekere mate rekening is gehouden dat er mogelijke meerdere activiteiten door belastingplichtige kunnen worden uitgevoerd. (tot 3 activiteiten). Daaraan is per finr het aantal auto's gekoppeld en de selectie gemaakt op resp. 10 en 25 auto's zoals eerder beschreven. Opmerkelijk dat dan nog maar 11.422 finrs resteren. Deze finrs behoren toe aan 10.451 entiteiten. **Wijziging: als gevolg van de opschaling naar minimaal 25 auto's in een van de jaren 2015 t/m 2017 zijn er nu 9.957 entiteiten geselecteerd. Daarvan behoren er 3.043 toe aan de kantoren Leeuwarden, Groningen, Emmen, Enschede, Almere en Zwolle.**

Telling op entiteitniveau

Voor deze verkenning "autohandel" is gebruik gemaakt van het entiteitenbestand van mei 2018. Daarin staan de actieve entiteiten opgenomen. In totaal zijn er dus 9.957 entiteiten bekend met een branchecode autohandel volgens de definitie uit tabel 3 die tevens voldoen aan de minimale eisen van 25 verkochte auto's. De verdeling van de entiteiten over de kantoren en segmenten is opgenomen in tabel 7. De verdeling over de aandachtsgebieden staat in tabel 8.

Tabel 7

Telling van Locatie/ segment	MKB	CNV	VIP	GRO	Eindtotaal
Almere	425	5	1		431
Emmen	443	16			459
Enschede	587	13	1	10	611
Groningen	344	10		11	365
Leeuwarden	520	23			543
Zwolle	580	30	2	22	634
Eindtotaal	**2.899**	**97**	**4**	**43**	**3.043**

Tabel 8 Verdeling entiteiten over de kantoren en aandachtgebieden.

Telling van Locatie/aandachtgebied	H&TR	KO	AR&D	VG&L	GRO	Eindtotaal
Almere	209	199	16	7		431
Emmen	236	197	20	6		459
Enschede	335	251	10	5	10	611
Groningen	174	162	12	6	11	365
Leeuwarden	287	234	11	11		543
Zwolle	320	262	21	9	22	634
Eindtotaal	**1.561**	**1.305**	**90**	**44**	**43**	**3.043**

Samenloop HSB bestanden en branche indeling autohandel

Om te komen tot een groep autohandelaren is er voor gekozen om het object auto leadend te laten zijn in combinatie met de branchecode. Er is een indeling gemaakt over het gemiddeld aantal verkochte auto's in de jaren 2015 t/m 2017, op entiteitniveau. De indeling is per kantoor (tabel 9), per brancheomschrijving (tabel 10), per segment (tabel 11) en aandachtsgebied (tabel 12)

Tabel 9 Verdeling kantoren

Locatie en gem. aantal verk. 15_17	a < 25	b > 25 < 100	c > 100 < 250	d > 250 < 500	e > 500 < 1000	f > 1000	Eindtotaal
Almere	63	177	124	39	21	7	431
Emmen	59	200	112	55	17	16	459
Enschede	75	270	158	61	32	15	611
Groningen	35	167	105	35	11	12	365
Leeuwarden	51	262	136	59	17	18	543
Zwolle	84	233	179	79	28	31	634
Eindtotaal	**367**	**1.309**	**814**	**328**	**126**	**99**	**3.043**

Tabel 10 Verdeling branches

Brcode	Omschrijving / gemiddelde verkopen 15	a < 25	b > 25 < 100	c > 100 < 250	d > 250 < 500	e > 500 < 1000	f > 1000	Eindtotaal
6622	Gebruikte personenauto's	131	530	362	155	50	24	1.252
6821	Autoreparatiebedrijven (garages) en de	83	348	198	69	19	14	731
6621	Nieuwe personenauto's	9	54	59	37	24	30	213
6187	Auto's, auto-accessoires en onderdelen	25	69	40	21	7	7	169
6387	Auto's, accessoires en onderdelen (ook	8	35	26	10	2	6	87
pm	Overige branchecodes (aantal 183)	111	273	129	36	24	18	591
Eindtotaal		**367**	**1.309**	**814**	**328**	**126**	**99**	**3.043**

Tabel 11 Verdeling per segment

Segment	a < 25	b > 25 < 100	c > 100 < 250	d > 250 < 500	e > 500 < 1000	f > 1000	Eindtotaal
MKB	362	1.275	778	304	114	66	2.899
CNV	4	27	30	21	10	5	97
VIP	0	1	1	2			4
GRO	1	6	5	1	2	28	43
Eindtotaal	**367**	**1.309**	**814**	**328**	**126**	**99**	**3.043**

Tabel 12 Verdeling aandachtsgebieden

Aandachtsgeb.	a < 25	b > 25 < 100	c > 100 < 250	d > 250 < 500	e > 500 < 1000	f > 1000	Eindtotaal
H&TR	83	560	497	253	104	64	1561
KO	271	689	277	59	9		1305
AR&D	6	36	25	9	8	6	90
VG&L	6	18	10	6	3	1	44
GRO	1	6	5	1	2	28	43
Eindtotaal	**367**	**1309**	**814**	**328**	**126**	**99**	**3043**

Omzet voor de OB 2015-2017

In tabel 13 staat de omzet OB behorende bij de entiteiten van de 6 pilotkantoren met de verdeling over de 5 belangrijkste autobranchecodes en overige branches. De omzetcijfers zijn exclusief Groot Ondernemingen. Omdat de omzet op entiteitniveau is weergegeven kunnen ook activiteiten die niet auto gerelateerd zijn van invloed zijn. Daarnaast dragen stakende en startende ondernemingen bij aan de fluctuaties. Er is een groei zichtbaar van 2015-2017 van 7%. De hoogste groei is zichtbaar bij de handel in gebruikte personenauto's en handel in auto's , autoaccessoires onderdelen en banden.

Tabel 13

Br.code	Omschrijving	Aantal Dosnr	Omzet OB2015	Omzet OB2016	Omzet OB2017	% groei
6622	Gebruikte personenauto's	1.252	792.135.228	858.514.683	911.629.588	115%
6821	Autoreparatiebedrijven (ga	728	674.445.322	705.870.642	739.790.598	110%
6621	Nieuwe personenauto's	195	892.799.022	806.096.526	827.159.263	93%
6187	Auto's, auto-accessoires en	166	220.809.060	258.710.769	278.368.163	126%
6387	Auto's, accessoires en onde	85	202.165.302	199.938.028	226.033.437	112%
PM	Overige branchecodes 178	574	744.473.357	764.232.605	803.407.453	108%
Eindtotaal		**3.000**	**3.526.827.291**	**3.593.363.253**	**3.786.388.502**	**107%**

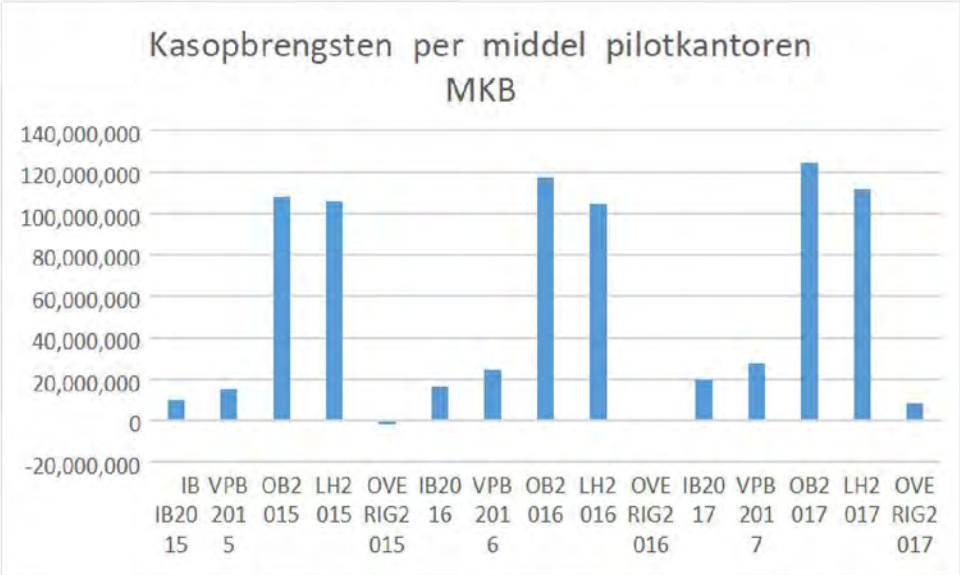
Kasstroom 2015-2017

De kasstroom bestaat uit het totaal van de betaalde belastingen IH, LH, OB, VPB en overige middelen in de genoemde jaren. Duidelijk zichtbaar is dat Kleine Ondernemingen maar zeer beperkt bijdraagt aan de totale kasstroom, maar in aantallen wel een substantieel deel van de doelgroep vormt. Grote Ondernemingen draagt met 88 % van de kasstroom het meeste bij.

Aandachts gebied	Aantal Dosnr	Omzet OB2015	Omzet OB2016	Omzet OB2017	Aandeel in omzet 2017	Aandeel in aantal	% groei 2015-2017
H&TR	1.561	3.023.718.198	3.083.655.115	3.255.287.686	86%	52%	108%
KO	1.305	133.663.875	144.511.145	159.642.074	4%	44%	119%
AR&D	90	245.355.691	233.849.980	234.290.718	6%	3%	95%
VG&L	44	124.089.527	131.347.013	137.168.024	4%	1%	111%
Eindtotaal	**3.000**	**3.526.827.291**	**3.593.363.253**	**3.786.388.502**	**100%**	**100%**	**107%**

Kasstroom per middel, verdeeld over MKB Midden en KO

De kasopbrengsten per middel van de 3.000 entiteiten is weergegeven in onderstaande tabel. Het middel OB en LH vormen het grootste deel van de kasopbrengsten.



Kasstroom verdeeld per middel over MKB midden en KO verdeeld over de 4 risicogroepen

De entiteiten kunnen verdeeld worden in 4 groepen, met de indicatoren Belang (Groot/Klein)en risico (Groot/Klein). Deze zijn gerelateerd aan een kasstroom van meer/minder dan € 100.000 en een aandachtscategorie van A-B dan wel C-D. Duidelijk zichtbaar is dat de groep entiteiten met Belang Groot in aantal 23 % vormt van het totaal, maar wel goed is voor 100 % van de kasstroom.

Belang/Risico	BGRG	BGRK	BKRG	BKRK	Overig	Eindtotaal	% Belang Groot
Aantal	436	255	1.012	1.224	73	3.000	23%
IB2015	5.928.055	2.774.983	2.088.970	-314.827	-104.902	10.372.279	
VPB2015	5.585.948	7.257.484	838.591	1.898.881	0	15.580.904	
OB2015	59.475.333	42.876.945	3.093.705	2.699.853	-9.526	108.136.310	
LH2015	50.683.763	37.113.368	8.551.272	9.648.577	11.733	106.008.713	
OVERIG2015	12.018.894	11.670.340	-7.523.472	-17.923.494	3.903	-1.753.829	
Totaal 2015	133.691.993	101.693.120	7.049.066	-3.991.010	-98.792	238.344.377	99%
IB2016	10.037.130	1.276.731	4.683.362	660.201	-121.483	16.535.941	
VPB2016	9.715.995	10.327.880	2.009.886	2.747.548	0	24.801.309	
OB2016	66.557.448	50.141.230	-1.358.678	1.928.819	81.701	117.350.520	
LH2016	50.433.052	36.541.158	8.207.835	9.502.828	25.995	104.710.868	
OVERIG2016	12.846.108	11.255.175	-13.132.325	-11.000.572	22.186	-9.428	
Totaal 2016	149.589.733	109.542.174	410.080	3.838.824	8.399	263.389.210	98%
IB2017	12.457.803	1.840.089	5.416.732	200.104	-1.821	19.912.907	
VPB2017	12.955.072	9.098.924	1.989.094	3.459.273	0	27.502.363	
OB2017	77.344.806	53.652.878	-4.249.104	-2.216.953	39.711	124.571.338	
LH2017	54.581.208	38.745.305	8.603.745	9.433.654	119.730	111.483.642	
OVERIG2017	22.211.215	19.562.088	-10.940.990	-22.456.915	54.084	8.429.482	
Totaal 2017	179.550.104	122.899.284	819.477	-11.580.837	211.704	291.899.732	104%

Invordering mei 2018

In bijna 20 % van de gevallen komt een entiteit voor in de invordering. Opvallend is het hoge openstaande bedrag bij kantoor Zwolle. Van de 10 hoogste bedragen invordering zijn er 8 van kantoor Zwolle. Een relatie met hoge correcties bij ingestelde boekenonderzoeken ligt voor de hand.

Locatie	Aantal zonder Inv.	Aantal met Inv.	% invordering	Open Bedrag Inv	Cons. Aansl en Aansprst	Beinvloedbaar Inv	Beperkt_Beinvloedbaar Inv	Niet_Beinvloedbaar Inv	Aantal Aanslagen Open
Almere	335	96	22%	3.512.105	563.835	1.199.796	120.723	1.627.751	852
Emmen	369	90	20%	4.231.867	374.184	3.123.855	279.392	454.436	719
Enschede	494	107	18%	1.585.215	0	1.061.316	186.820	337.079	635
Groningen	274	80	23%	3.494.443	373.219	1.606.079	2.998	1.512.147	540
Leeuwarden	461	82	15%	2.332.943	78.853	1.540.170	8.536	705.384	881
Zwolle	491	121	20%	40.082.968	598.816	24.326.589	7.379.621	7.777.943	3913
Eindtotaal	2424	576	19%	55.239.541	1.988.907	32.857.805	7.978.090	12.414.739	7540

Het gemiddeld openstaand bedrag is hoog bij met name Arbeid en Dienstverlening en Vastgoed en Landbouw.

Aandachtgebied	Aantal zonder Inv.	Aantal met Inv.	% invordering	Open Bedrag Inv	Cons. Aansl en Aansprst	Beinvloedbaar Inv	Beperkt_Beinvloedbaar Inv	Niet_Beinvloedbaar Inv	Aantal Aanslagen Open	Gemiddeld per entiteit
H&TR	1262	299	19%	32.910.679	1.617.869	16.288.261	6.728.823	8.275.726	3.196	110.069
KO	1071	234	18%	1.354.512	69	899.282	83.764	371.397	1.660	5.789
AR&D	63	27	30%	11.778.316	370.969	7.271.842	1.076.360	3.059.145	1.682	436.234
VG&L	28	16	36%	9.196.034	0	8.398.420	89.143	708.471	1.002	574.752
Eindtotaal	2424	576	19%	55.239.541	1.988.907	32.857.805	7.978.090	12.414.739	7.540	95.902

Juist en volledig 2016 en 2017 veldtoets

In dit onderdeel wordt gerapporteerd over de afgedane boekenonderzoeken, code 50. De onderzoeksresultaten komen uit IKB. Uitgangspunt is het bestand met 10.451 entiteiten, waarin autohandel met de 5 branchecodes geraakt wordt. Er zijn diverse mogelijkheden:

1. Entiteiten (met en zonder autohandel) met finrs met en zonder autohandel activiteiten, betrokken in onderzoek
2. Entiteiten (met en zonder autohandel) met finrs, enkel met autohandelactiviteiten, betrokken in onderzoek
3. Entiteiten (enkel autohandel) met finrs met en zonder autohandel activiteiten, betrokken in onderzoek
4. Entiteiten(enkel autohandel) met finrs enkel autohandel activiteiten , betrokken in onderzoek

In deze rapportage richt ik mij op het toezicht op finr. niveau met enkel correcties in de autohandel, ongeacht waar de entiteit is ingedeeld; dus situatie 2.

Er zijn in de periode 2013 t/m april 2018 ongeveer 2.500 boekenonderzoeken heffing afgedaan. De opbrengsten zijn ingaande het jaar 2015 fors gestegen t.o.v. van de voorafgaande jaren. Ook het changepercentage is toegenomen.

Jaar af onderzoek	2013	2014	2015	2016	2017	2018	Eindtotaal
Totale correctie	510.597	3.727.244	23.870.254	21.144.558	42.631.429	7.284.484	99.168.566
Aantal onderzoeken	139	374	537	647	602	225	2.524
Gemiddelde corr	3.673	9.966	44.451	32.681	70.816	32.375	39.290
Aantal onderz.zonder corr.	99	224	257	274	238	89	1.181
Aantal onderz.met corr.	40	150	280	373	364	136	1.343
Percentage Change	29%	40%	52%	58%	60%	60%	53%

De verdeling over de kantoren

Kantoor	Correctie Ja	Totaal correctie	Correctie Nee	Totaal af 2013_2016	% change	Gem opbrengst
ALMELO	2	50.244	1	3	67%	16.748
ALMERE	46	762.557	38	84	55%	9.078
AMSTERDAM	30	4.652.790	18	48	63%	96.933
ARNHEM	68	3.885.894	66	134	51%	28.999
BREDA	116	6.435.088	92	208	56%	30.938
BUITENLAND	2	-2.485	8	10	20%	-249
DEN HAAG	67	6.441.622	53	120	56%	53.680
DOETINCHEM	34	2.081.558	35	69	49%	30.168
EINDHOVEN	134	22.058.856	106	240	56%	91.912
EMMEN	60	2.695.825	50	110	55%	24.508
ENSCHEDE	77	4.654.208	88	165	47%	28.207
GRONINGEN	47	2.084.548	39	86	55%	24.239
HEERLEN			2	2	0%	0
HOOFDDORP	69	4.666.849	60	129	53%	36.177
HOORN	67	3.773.327	59	126	53%	29.947
LEEUWARDEN	65	1.814.828	51	116	56%	15.645
MAASTRICHT	72	2.405.742	83	155	46%	15.521
MIDDELBURG	35	2.251.395	29	64	55%	35.178
ROTTERDAM	102	2.933.654	112	214	48%	13.709
UTRECHT	110	13.085.223	62	172	64%	76.077
VENLO	54	3.300.676	74	128	42%	25.787
ZWOLLE	86	9.136.167	55	141	61%	64.796
Eindtotaal	1343	99.168.566	1181	2524	53%	39.290

Top op basis van hoogst aantal afgedane projecten 2017

PR.CODE	Naam project	Aantal van 2016	Aantal van 2017	Som van 2016	Som van 2017	Gem. corr 2016	Gem. corr 2017
Eindtotaal		647	602	21.144.558	42.631.429	32.681	70.816
2075	Autohandel	101	162	2.476.641	7.524.760	24.521	46.449
1073	OB negatief (NNO-box)	72	36	751.093	421.394	10.432	11.705
3940	Steekproef ondernemingen 2017		21		106.204	#DEEL/0!	5.057
3952	BTW Carrouselfraude Prio 2		20		961.808	#DEEL/0!	48.090
8498	Boekenonderzoekenn.a.v.individu	23	17	1.276.724	2.279.137	55.510	134.067

Top 5 op basis van hoogst scorende gemiddelde

PR.CODE	Naam project	Aantal van 2016	Aantal van 2017	Som van 2016	Som van 2017	Gem. corr 2016	Gem. corr 2017
Eindtotaal		647	602	21.144.558	42.631.429	32.681	70.816
3954	BTW Carrouselfraude Controleverzoeken FIOD		5		4.860.468	#DEEL/0!	972.094
3950	BTW Carrouselfraude SCAC: FIOD		6		4.570.624	#DEEL/0!	761.771
7002	DoorRegiogeselecteerdeonderzoek	6	5	150.340	3.790.416	25.057	758.083
1176	RIEC: Cannabis	3	5	527.675	3.053.148	175.892	610.630
3023	Mismatches (ICP EU BTW-pakket 20	7	1	297.232	319.722	42.462	319.722
1170	RIEC: Woonwagencentra	2	2	19.726	501.478	9.863	250.739

Top 5 op basis van hoogste opbrengst per project

PR.CODE	Naam project	Aantal van 2016	Aantal van 2017	Som van 2016	Som van 2017	Gem. corr 2016	Gem. corr 2017
Eindtotaal		647	602	21.144.558	42.631.429	32.681	70.816
2075	Autohandel	101	162	2.476.641	7.524.760	24.521	46.449
3954	BTW Carrouselfraude Controleverzoeken FIOD		5		4.860.468	#DEEL/0!	972.094
3950	BTW Carrouselfraude SCAC: FIOD		6		4.570.624	#DEEL/0!	761.771
7002	DoorRegiogeselecteerdeonderzoek	6	5	150.340	3.790.416	25.057	758.083
1176	RIEC: Cannabis	3	5	527.675	3.053.148	175.892	610.630

Risico indeling

Fiscaal dienstverlener

Er zijn ongeveer …… fiscaal dienstverleners actief in de autohandel. Ze verzorgen voor ,,,,, finrs de aangiften; dat is voor ,,,,, entiteiten . In ongeveer ….. entiteiten komen meerdere beconnummers voor. Van ….. entiteiten is niet bekend of ze gebruik maken van een fiscaal dienstverlener. Uit onderstaande tabel is af te leiden dat ..% van de fiscaal dienstverleners … % van de aangiften verzorgt. Verdiepende vraag: is er een relatie tussen het aantal klanten van de fiscaal dienstverlener en de compliance bij de ondernemingen.

Klanten	Aantal Becon	Aantal bel.pl
Klasse 50 -300	42	3.578
Klasse 25-49	150	5.015
Klasse 10-24	795	11.341
Klasse1-9	8.527	23.739
Totaal	9.514	43.673

Inzicht gebruik fiscaal dienstverlener op entiteitniveau

Ongeveer .. % van de entiteiten in H & TR (MKB midden) hebben een fiscaal dienstverlener; de entiteiten die vallen onder Kleine Ondernemingen daarentegen maar … %. . GO heeft in …% van de gevallen een fiscaal dienstverlener.

Externe informatie

BOVAG en RAI publiceren ook kerncijfers. Een aantal tabellen uit de publicatie Kerncijfers Auto en Mobiliteit 2018 zijn in de bijlagen opgenomen.

Verkoop gebruikte personenauto's							
Bron: RDC BOVAG	2011	2012	2013	2014	2015	2016	2017
Autobedrijven			1.032.088	1.048.593	1.091.258	1.139.932	1.146.654
Particulieren			762.258	742.383	759.228	805.186	830.849
Totaal			1.794.346	1.790.976	1.850.486	1.945.118	1.977.503

Registraties bestelauto's verkopen							
Bron: RDC RAI	2011	2012	2013	2014	2015	2016	2017
Totaal			50.568	51.761	57.702	70.398	73.478

Individuele import personenauto's naar brandstofsoort							
Bron: RDC BOVAG	2011	2012	2013	2014	2015	2016	2017
Benzine		46.739	63.351	81.500	104.614	124.475	144.019
Diesel		30.984	32.139	34.735	40.358	45.416	57.660
Hybride		1.122	2.467	2.543	5.986	7.776	5.517
LPG		926	641	743	811	913	847
Elektrisch		118	107	257	370	299	699
Aardgas		270	102	138	303	265	385
Biobrandstof		29	40	62	102	124	189
Waterstof		-	2	4	4	5	12
Totaal		80.188	98.849	119.982	152.548	179.273	209.328

Diefstalontwikkeling motorvoertuigen							
Bron: Stichting Aanpak Vo	2011	2012	2013	2014	2015	2016	2017
Personenauto's	11.658	11.396	11.761	10.712	10.091	9.179	8.257
Bedrijfsvoertuigen	2.355	2.427	2.689	2.383	1.877	1.912	1.630
Aanhangers/Opleggers	1.155	1.173	1.153	1.140	901	750	694
Motorrijwielen	1.996	1.807	1.963	1.753	1.845	1.579	1.631
Brom- en snorfietsen	16.869	16.183	14.487	14.693	14.504	12.698	11.383
Totaal	34.033	32.986	32.053	30.681	29.218	26.118	23.595

Werkgelegenheid in de mobiliteitsbranche							
Aantal per 1 januari	2011	2012	2013	2014	2015	2016	2017
Totaal werkgevers met personeel			11.700	11.500	11.550	11.550	11.450
Autobedrijven			54.708	52.307	50.841	52.271	51.183
Truckdealerbedrijven			7.957	8.246	7.163	7.296	7.231
Tweewielerbedrijven			8.176	8.354	8.654	9.327	8.832
Autoverhuurbedrijven			1.466	1.606	1.546	1.541	1.396
Bergingsbedrijven			620	598	587	601	581
Caravanbedrijven/Aanhangwagenbedrijven			1.191	1.161	1.129	1.169	1.125
Motorenrevisiebedrijven			484	497	506	518	505
Tankstations/Autowasbedrijven			17.180	17.000	16.650	16.050	17.000
Totaal werknemers			91.782	89.769	87.076	88.773	87.853

Export personenauto's naar brandstofsoort							
Bron: RDC BOVAG	2011	2012	2013	2014	2015	2016	2017
Diesel		167.525	136.465	108.411	104.045	116.791	111.445
Benzine		138.285	124.034	120.526	121.083	101.150	105.656
Hybride		5.130	6.061	5.567	4.896	6.041	9.075
LPG		13.140	11.183	10.397	9.561	9.030	7.991
Elektrisch		68	424	953	1.064	557	648
Aardgas		37	91	204	194	238	401
Biobrandstof		13	20	37	40	27	18
Totaal		324.198	278.278	246.095	240.883	233.834	235.234

Voorschrift Beveiliging Infrastructuur 2006
Normenset en maatregelen

VBI 2006

Belastingdienst

mei 2006

Inhoudsopgave VBI

0 Metagegevens 3
0.1 Documentgegevens 3
0.2 Opdrachtgegevens 3
0.3 Totstandkoming 3

1 Inleiding 5
1.1 Waarom dit handboek? 5
1.2 Verantwoordelijkheid voor het VBI 7
1.3 De relatie tussen het VBI en de domeinarchitectuur beveiliging 7
1.4 Opbouw van dit document 8
1.5 Afwijken van de maatregelenset 9
1.6 Overzicht van de wijzigingen in het VBI 9

2 Basis beveiligingsniveau 10
2.1 Identity and Access Management 10
2.1.1 Wat is identity and access management? 10
2.1.2 Hoe moet een ICT-systeem gebruikers identificeren en authenticeren? 12
2.1.3 Hoe moet een ICT-systeem gebruikers toegang verlenen? 16
2.2 Security Monitoring 20
2.2.1 Wat is security monitoring? 20
2.2.2 Welke informatie moet in een logbestand worden vastgelegd? 21
2.2.3 Hoe moeten onregelmatigheden in het logbestand worden vastgesteld? 24
2.2.4 Hoe moet vastgesteld worden dat de beveiliging juist gefunctioneerd heeft? 25
2.3 Encryption 27
2.3.1 Wat is encryption? 27
2.3.2 Wanneer moet encryptie worden toegepast? 28
2.3.3 Waaraan moet de encryptie voldoen? 30
2.3.4 Hoe moet het sleutelbeheer geregeld worden? 32
2.4 Boundary Protection 33
2.4.1 Wat is boundary protection? 33
2.4.2 Hoe moeten externe verbindingen worden beveiligd? 34
2.4.3 Welke zonering en compartimentering moet worden toegepast? 36
2.5 Business Continuity 39
2.5.1 Wat is business continuity? 39
2.5.2 Hoe moet de continuïteit van ICT-systemen worden gewaarborgd? 39

0 Metagegevens

0.1 Documentgegevens

Naam document	Voorschrift Beveiliging Infrastructuur 2006
Ook bekend als	VBI 2006
Versie	1.0 (status voor akkoord aangeboden)
Datum laatste wijziging	8 mei 2006
Vindplaats elektronische versie	Approw50\Algemeen\BDS1821 LTB\2210 VBI vernieuwen\Laatste versie\VBI 2006 v1.0.doc

0.2 Opdrachtgegevens

Er hebben twee opdrachten ten grondslag gelegen aan de totstandkoming van dit document, namelijk 'Uitwerken concept VBI', waarvoor 23 februari 2005 een verkorte offerte is uitgebracht en 'Afronden en formaliseren VBI'.

Opdracht

Opdrachtnummer	O-0209-006
Opdrachtomschrijving	Uitwerken Concept VBI
Start	1 maart 2005
Eind	31 december 2005

Opdracht

Opdrachtnummer	O-0412-005
Opdrachtomschrijving	Afronden en formaliseren VBI
Start	2 januari 2006
Eind	31 mei 2006

Opdrachtgever

Naam	Organisatie-onderdeel	**Rol**
Persoonsgegevens	B/CPP-GIS	Persoonsgegevens
Persoonsgegevens	B/CICT-AR	Persoonsgegevens

Het feit dat hier twee opdrachtgevers vermeld staan, heeft te maken met de verantwoordelijkheid voor het VBI. B/CPP is verantwoordelijkheid voor het aanreiken van richtlijnen en normen waaraan de infrastructuur van B/CICT dient te voldoen. De vertaling van normen in de te realiseren beveiligingsmaatregelen is de verantwoordelijkheid van B/CICT. Zowel de richtlijnen, als de normen, als ook de maatregelen zijn als samenhangend geheel in het VBI beschreven.

Formele goedkeuring

Naam	Goedkeuring op	**Datum**
MT B/CPP	Richtlijnen en normen. De maatregelen zijn ter kennisname	April 2006
Stuurgroep Beveiliging B/CICT	Maatregelen en algemene documentstructuur. Richtlijnen en normen ter kennisname	13 Juni 2006

0.3 Totstandkoming

Auteur

Naam	Organisatie-onderdeel	Rol
Persoonsgegevens	B/CICT-AR	Persoonsgegevens

Reviewers

Naam	Organisatie-onderdeel	Rol	Akkoord
Persoonsgegevens	B/CPP-GIS	Persoonsgegevens	Akkoord
	B/CPP-GIS		Akkoord
	B/CICT-CO		Akkoord
	B/CICT-AR		Akkoord
	B/CICT-EX		Akkoord
	B/CICT-AR		Akkoord
	B/CPP-GIS		Akkoord
	B/CPP-GIS		Akkoord
	B/CICT-AR		Akkoord
	B/CICT-ON		Akkoord
	B/CICT-CO		Akkoord
	B/CICT-AR		Akkoord
	B/CICT-AR		Akkoord
	B/CICT-AR		Akkoord
	B/CICT-CO		Akkoord

1 Inleiding

1.1 Waarom dit handboek?

De primaire en ondersteunende processen van de Belastingdienst zijn in hoge mate afhankelijk van adequate informatievoorziening en betrouwbare ICT-Services. Daarom is het informatie-beveiligingsbeleid van de Belastingdienst er op gericht om gemeenschappelijk gebruik van informatie mogelijk te maken, terwijl de betrouwbaarheid van de informatievoorziening gewaarborgd blijft.

De betrouwbaarheid van de informatievoorziening valt uiteen in:
1. **Beschikbaarheid**: zekerstellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers;
2. **Integriteit**: het waarborgen van de correctheid en de volledigheid van informatie en computerprogrammatuur;
3. **Vertrouwelijkheid**: het beschermen van gevoelige informatie tegen ongeautoriseerde kennisname.

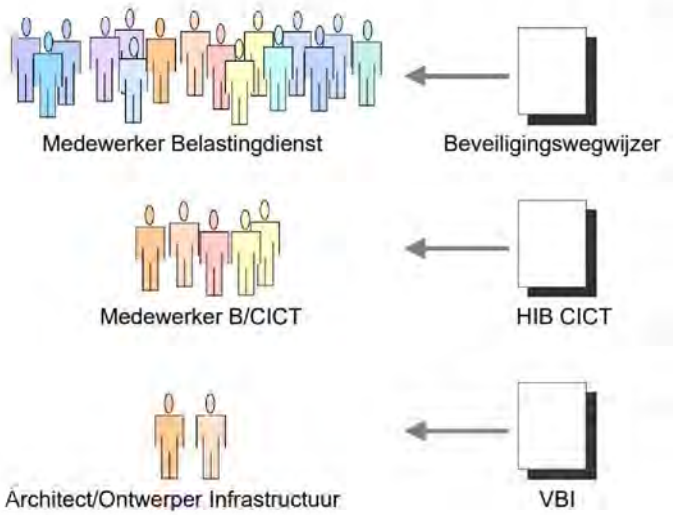
Het VBI bevat de gemeenschappelijke infrastructurele producteisen

Om een beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen. Dit handboek, het Voorschrift Beveiliging Infrastructuur (VBI), beschrijft een specifiek deel van deze gemeenschappelijke uitgangspunten, namelijk de infrastructurele producteisen die gelden bij het voortbrengen van ICT-services. Dit wordt niet in andere handboeken geadresseerd. In de volgende tabel staan een aantal geldende handboeken op het gebied van beveiliging genoemd.

Regelgeving beveiliging	Doelgroep	Inhoud	Voorbeeld van een maatregel
Handboek InformatieBeveiliging – Basis Beveiligings-Niveau Belastingdienst (HIB-BBN)	M1-Kantoren en Medewerkers op het gebied informatie-beveiliging	Te treffen maatregelen binnen de processen van Belastingdienstkantoren	Het management maakt gebruik van een procedure (checklist) 'Uitstroom Medewerker'.
Beveiligingswijzer	Medewerkers van een Belastingdienstkantoor	Maatregelen uit HIB-BBN vertaald naar de medewerkers van een kantoor.	Bij einde dienstverband of verplaatsing naar een ander kantoor moet je de belasting-dienstkaart op de laatste werkdag inleveren bij je HRM.
Handboek Calamiteitenbeheer (HCB)	Verantwoordelijk management binnen een Belastingdienst-kantoor en de bedrijfs-hulpverleners (BHV-ers)	Uitvoering van het HCB leidt tot een viertal deelplannen: 1. het Preventieplan 2. het Crisismanagementplan 3. het BHV- en ontruimingsplan 4. het Continuïteitsplan	Het crisisteam moet te allen tijde geformeerd kunnen worden. Dat betekent dat zowel binnen als buiten kantoortijden altijd minimaal één van de leden bereikbaar is.
Handboek Informatie-Beveiliging B/CICT (HIB CICT)	Medewerkers B/CICT	Procesmaatregelen binnen de processen van B/CICT	Naar de acceptatietestomgeving en exploitatieomgeving overgedragen programmatuur kan niet meer gewijzigd worden.
Voorschrift Beveiliging Applicaties (VBA)	Ontwerpers en architecten van B/CICT	Algemene producteisen voor applicaties	Applicatietaken voor het opvoeren van stamgegevens en het opvoeren van mutatiegegevens zijn gescheiden.
Voorschrift Beveiliging Infrastructuur (VBI)	Ontwerpers en architecten van infrastructuur bij B/CICT	Algemene producteisen voor technische infrastructuur.	Gebruikers worden door het systeem gedwongen een initieel wachtwoord te wijzigen bij de eerste aanmelding.

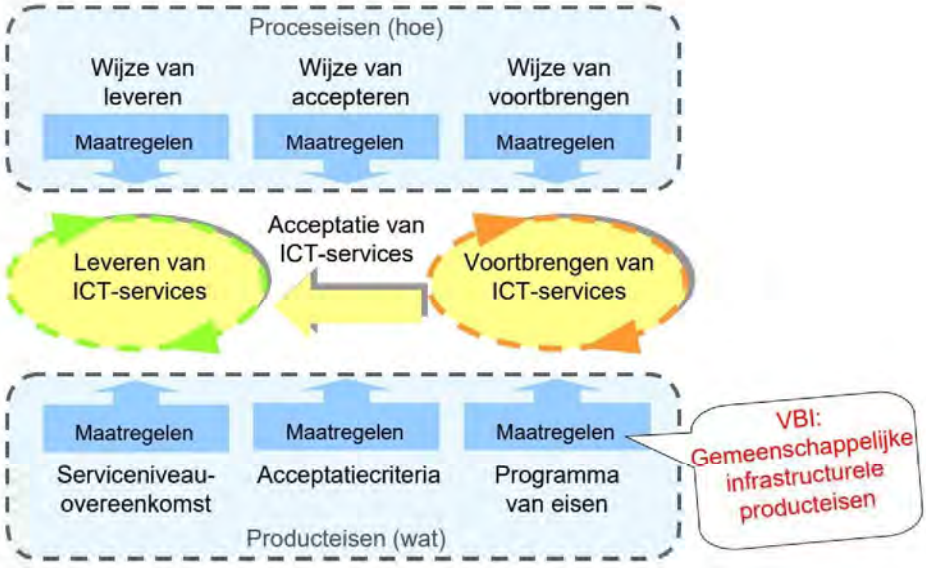
De handboeken vullen elkaar aan. Het VBI heeft dus een eigen doelgroep en een bestaansgrond naast de andere handboeken.

Een ontwerper/architect van infrastructuur bij B/CICT heeft te maken met meerdere handboeken omdat de ontwerper/architect én een medewerker van de Belastingdienst is én een medewerker van B/CICT is én een medewerker is in de functie van ontwerper of architect.



Figuur 1: Een ICT-Ontwerper is een medewerker van B/CICT en van de Belastingdienst

Vanuit deze rollen zijn in essentie drie beveiligingsvoorschriften van belang: de Beveiligingswijzer, het HIB CICT en het VBI. De meest recente versie van deze documenten is te vinden via de startpagina van ICT-net in de sectie Organisatie onder de kop Beveiliging. In de beveiligingswijzer staat hoe je je als medewerker van de Belastingdienst dient te gedragen. In het HIB CICT staat op welke wijze ICT-services ontwikkeld, geaccepteerd en geleverd moeten worden. Dit zijn dus proceseisen. In het VBI staat aan welke inhoudelijke beveiligingseisen te ontwikkelen infrastructuur altijd dient te voldoen. Dit zijn de gemeenschappelijke infrastructurele producteisen.



Figuur 2: Proceseisen versus producteisen

VBI bevat het Basis beveiligingsniveau

De eisen, en daarmee ook de beveiligingseisen, die gesteld worden door de opdrachtgever aan een voort te brengen ICT-service zijn gespecificeerd in het Programma van Eisen. Door in het Programma van Eisen te verwijzen naar het VBI hoeven de beveiligingseisen die altijd gelden, het basis beveiligingsniveau, niet iedere keer gespecificeerd te worden.

Een PVE bevat aanvullende beveiligingseisen

Voor wat betreft de beveiligingseisen kan het programma van eisen zich dan beperken tot het specificeren van beveiligingseisen die boven het basis beveiligingsniveau uitkomen. Dit zijn de aanvullende beveiligingseisen.

1.2 Verantwoordelijkheid voor het VBI

Het VBI wordt actueel gehouden, zodat het VBI de *beveiligingskaders* weergeeft zoals die momenteel gelden om het huidige gedefinieerde *basis beveiligingniveau* te realiseren.

Actualiseren van richtlijnen en normen

Het basis beveiligingsniveau is beschreven in termen van richtlijnen en normen. Het gewenste basis beveiligingsniveau zal gelijke tred moeten houden met de toenemende mate waarin de Belastingdienst afhankelijk is van de informatievoorziening en ontwikkelingen in onder meer wetgeving en maatschappelijke standaards. De verantwoordelijkheid voor het actualiseren van het gewenste basis beveiligingsniveau is belegd bij B/CPP-GIS.

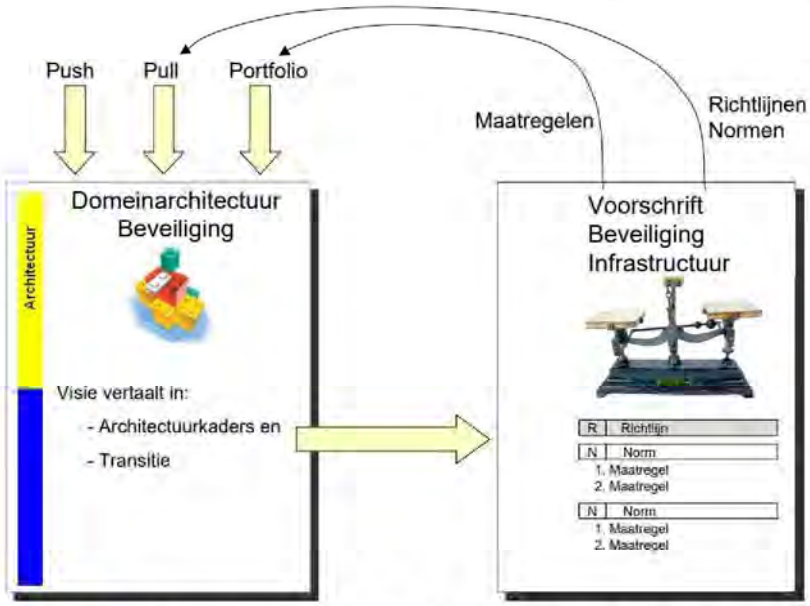
Actualiseren van maatregelen

Het beveiligingskader is beschreven in termen van maatregelen. De invulling van het beveiligingsniveau door beveiligingsmaatregelen zal onder meer wijzigen door het bekend worden van kwetsbaarheden. Denk hierbij bijvoorbeeld aan het beschikbaar komen van kennis en hulpmiddelen om beveiliging te doorbreken. De betrouwbaarheid van de informatievoorziening neemt dan af en de beveiligingsrisico's nemen toe. Om hetzelfde beveiligingsniveau te realiseren zullen er meer of betere maatregelen genomen moeten worden. De verantwoordelijkheid voor het definiëren en onderhouden van deze beveiligingskaders is belegd bij de B/CICT-AR (zie ook HIB CICT AR N-1-1). De penvoering over het VBI is eveneens belegd bij B/CICT-AR. Dit omdat maatregelen frequenter zullen wijzigen dan de richtlijnen en normen, en omdat een wijziging in richtlijnen en normen altijd een heroverweging van maatregelen tot gevolg heeft. Veranderingen in het beveiligingskader worden geïnitieerd vanuit de domeinarchitectuur beveiliging. In de volgende paragraaf wordt hierop ingegaan.

1.3 De relatie tussen het VBI en de domeinarchitectuur beveiliging

De DA beveiliging is input voor het VBI

De domeinarchitectuur beveiliging geeft de visie weer op de verandering van beveiligingskaders op basis van wat er kan in de markt (push), de klantvraag (pull) en de huidige situatie (portfolio). De consequenties van veranderingen en de wijze waarop een verandering in gang wordt gezet, wordt weergegeven in de vorm van een transitieschema. De te hanteren beveiligingsmaatregelen in het VBI worden hierop aangepast. Het VBI is hier dus volgend en de domeinarchitectuur beveiliging is leidend. Het VBI omvat het gehele actuele beveiligingskader, terwijl de domeinarchitectuur primair ingaat op de veranderingen in het beveiligingskader.



Figuur 3: De relatie tussen de DA Beveiliging en het VBI

Het VBI is input voor de DA beveiliging

VBI is ook input voor de domeinarchitectuur: De richtlijnen en normen vormen een belangrijk onderdeel van de klantvraag en de maatregelen zijn input voor de huidige situatie. Deze input is noodzakelijk om wijzigingen in architectuurkaders te beperken. Geen revolutie maar evolutie is daarbij het credo.

1.4 Opbouw van dit document

Aandachtgebieden

Het basis beveiligingsniveau is in het VBI uitgewerkt voor de volgende aandachtsgebieden:

- Identity and Access Management (IAM)
- Security Monitoring (SM)
- Encryption (ENC)
- Boundary Protection (BP)
- Business Continuity (BC)

Ieder aandachtsgebied wordt in een separate paragraaf beschreven, waarbij in een inleiding het referentie- en begrippenkader van het aandachtsgebied wordt behandeld.
Deze aandachtsgebieden zijn gebaseerd op de beveiligingsfuncties uit de domeinarchitectuur beveiliging. Hieraan toegevoegd is het aandachtsgebied Business Continuity. Dit aandachtsgebied valt binnen de afbakening van de domeinarchitectuur beheer. Business Continuity is onderdeel van dit handboek, omdat informatiebeveiliging binnen de Belastingdienst en volgens de Code voor informatiebeveiliging (ISO/IEC 17799) wordt gekarakteriseerd als het waarborgen van zowel de vertrouwelijkheid en de integriteit, als ook de beschikbaarheid van de informatie.

De richtlijnen, normen en maatregelen zijn volgens de volgende structuur beschreven:

Niveau	Stramien	Omschrijving
Strategisch	Aandachtsgebied	Clustering van richtlijnen, normen en maatregelen die binnen het aandachtsgebied moeten worden getroffen. In een inleiding wordt ingegaan op het referentie- en begrippenkader van het aandachtsgebied.
	Richtlijn	Om onderscheid aan te brengen tussen richtlijnen wordt de volgende syntax gehanteerd: <aandachtsgebied R(ichtlijn) – volgnummer>. Richtlijnen zijn weergegeven in een opgevuld grijs kader.
	Risicoafweging	Tekstuele beschrijving van risico's die met de richtlijn worden afgedekt.
Tactisch	Norm	Normen zijn een nadere uitwerking van een richtlijn. Om onderscheid aan te brengen wordt de volgende syntax gehanteerd: <aandachtsgebied N(orm) – volgnummer – doorloopnummer>. Normen zijn weergegeven in een kader.
	Toelichting	Toelichting waarin de norm nader wordt gespecificeerd of waar uitzonderingen op de norm worden beschreven.
Operationeel	Maatregelen	Operationeel te treffen set van maatregelen die, uitgaande van een standaard risicoprofiel, in opzet tegemoet komen aan de gestelde norm. In tegenstelling tot het HIB-BBN Belastingdienst zijn maatregelen genummerd. Een opsomming binnen een maatregel is aangegeven met een kleine letter. Een maatregel kan daardoor exact aangeduid worden (formaat ZZZ N 9-9 9a), echter maatregelen zijn niet los te zien van de norm.

1.5 Afwijken van de maatregelenset

Verhoogde risico's

De richtlijnen en normen in het VBI beschrijven het basis beveiligingsniveau. Dit niveau is het minimale niveau dat de Belastingdienst hanteert voor de beveiliging in de infrastructuur. Dit basisniveau is in de meeste gevallen toereikend om beveiligingsrisico's tot een acceptabel niveau te beperken. In bijzondere situaties kan er echter sprake zijn van verhoogde risico's. Of hiervan sprake is, bepaalt het verantwoordelijke management. Dat kan worden vastgesteld door een risicoanalyse uit te voeren bij veranderingen. Daarnaast wordt jaarlijks de actualiteit van de generieke analyse van verhoogde risico's vastgesteld (zie HIB-BBN 2005 P&C N-1-2). Wanneer sprake is van verhoogde risico's dan dienen er aanvullende maatregelen genomen te worden, dat wil zeggen bovenop de maatregelen beschreven in het basis beveiligingsniveau.

Andere invulling van het basisniveau

Met andere beveiligingsmaatregelen dan de in het VBI beschreven maatregelen kan ook het basis beveiligingsniveau bereikt worden. De vertaling van de normen in maatregelen zou daarom als minder dwingend opgevat kunnen opvatten. Toch is dat niet zo. De samenhang en de eenduidigheid van de maatregelen binnen de gehele infrastructuur is in belangrijke mate bepalend voor het uiteindelijke gerealiseerde beveiligingsniveau. Is er dan geen mogelijkheid om af te wijken van de beschreven maatregelen? Toch wel, maar alleen met een goede reden en in overleg met de B/CICT AR-Beveiliging. De mogelijke beveiligingsrisico's die het afwijken van de voorgeschreven beveiligingsmaatregelen met zich mee brengt, worden daarbij in kaart gebracht middels een risicoanalyse.

1.6 Overzicht van de wijzigingen in het VBI

VBI 2006 is een nieuw ijkpunt

Deze paragraaf is gereserveerd om de onderdelen op te sommen die ten opzichte van de voorgaande versie gewijzigd zijn. Omdat het VBI 2006 ten opzichte van het VBI 1.0 uit 2002 integraal gewijzigd is, zijn de veranderingen niet opgenomen. Het VBI 2006 is als een nieuw ijkpunt te beschouwen.

2 Basis beveiligingsniveau

2.1 Identity and Access Management

2.1.1 Wat is identity and access management?

ICT is al lang niet meer de elektronische vervanging van formulieren en dossiers. In feite worden met behulp van ICT nieuwe ruimten gecreëerd, weliswaar elektronisch en virtueel, maar daarom niet minder werkelijk. In deze elektronische wereld moet alles een identiteit hebben. Anders kan het niet bestaan en niet meedoen in de elektronische wereld. Identity and Access Management (IAM) is de processen en de ondersteunende infrastructuur voor het creëren, onderhouden en gebruiken van deze elektronische identiteiten en de toegangsrechten tot de objecten binnen de elektronische wereld. Een object is hierbij hetgeen waar een subject iets mee wil doen. Een subject is een gebruiker gerepresenteerd door een gebruikersnaam. Een gebruiker kan daarbij een mens zijn, maar ook een ander ICT-systeem. Identity and Access Management omvat het identificeren, authenticeren en autoriseren.

Definitie Identity and Access Management

Identificeren

Bij het aanmelden op een systeem, ook wel inloggen genoemd, geeft de gebruiker de gebruikersnaam op waaronder hij/zij wil werken. Dit proces heeft identificeren. Feitelijk wordt met de gebruikersnaam de relatie gelegd tussen de gebruiker en de representatie van de identiteit op het systeem. Na het identificeren volgt doorgaans het authenticeren. Authenticeren is het vaststellen van de authenticiteit van gebruiker. Dit proces wordt uitgevoerd om te voorkomen dat een gebruiker zich kan voordoen als een andere gebruiker door simpel de gebruikersnaam van een ander te gebruiken. Om de authenticiteit van de gebruiker vast te stellen geeft de gebruiker een authenticiteitkenmerk op. Dat is iets dat alleen die gebruiker weet (bijvoorbeeld een wachtwoord), iets dat alleen die gebruiker bezit (bijvoorbeeld een smartcard), iets dat de gebruiker biometrisch kenmerkt (bijvoorbeeld een vingerafdruk), of een combinatie hiervan.

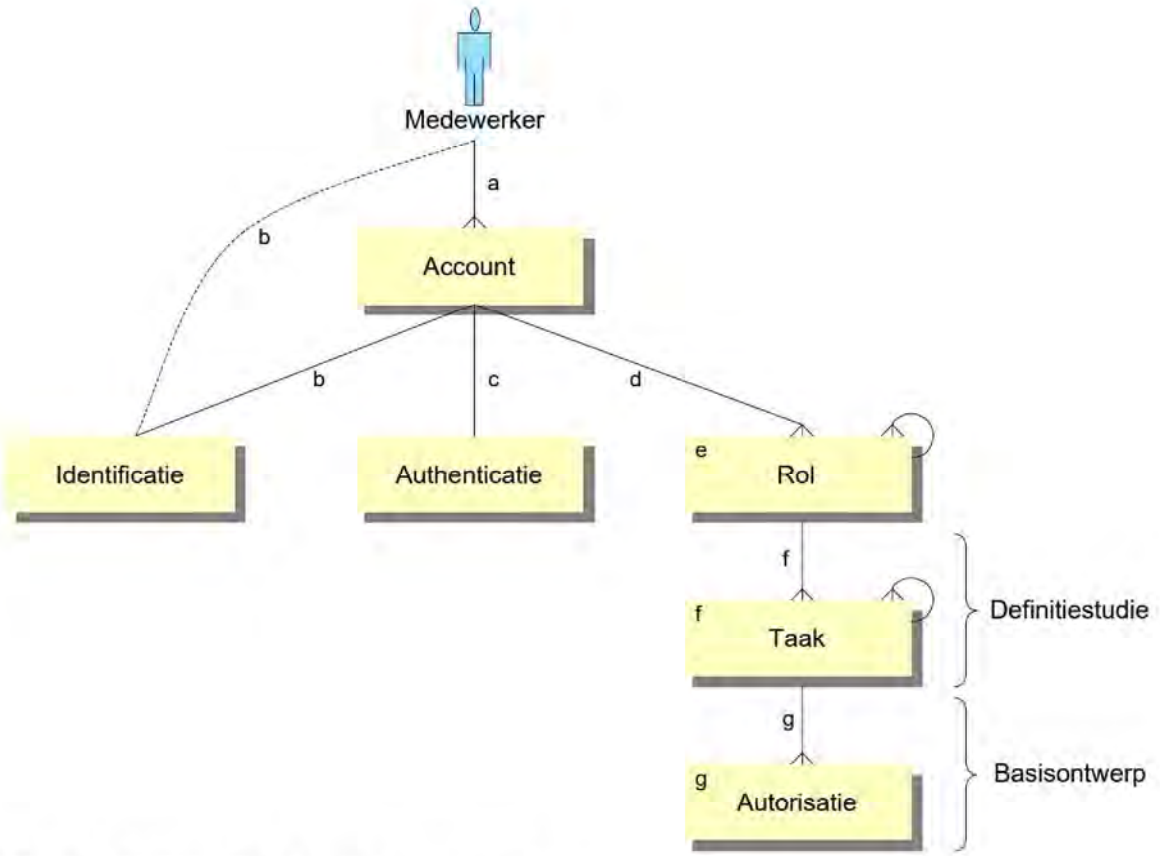
Authenticeren

Security context

Na een succesvolle aanmelding krijgt de gebruiker een security context van waaruit aan systeemprocessen opdrachten worden gegeven om handelingen op het ICT-systeem te verrichten. Een security context eindigt wanneer de sessie tussen de gebruiker en het systeem wordt beëindigd. Dat is wanneer de sessie verloopt, de gebruiker de sessie beeindigt (uitlogt), of wanneer een systeem de sessie beeindigt.
Een systeemproces dat de handelingen verricht voor de gebruiker heeft ook een eigen security context. Het systeemproces is namelijk ook een gebruiker. Het systeemproces verricht handelingen op het systeem binnen de security context van de gebruiker (impersonation) of binnen de security context van het systeemproces (delegation).

Autoriseren

Een gebruiker kan alleen handelingen op een systeem verrichten indien daarvoor de benodigde toegangsrechten zijn verleend. Toegangsrechten zijn synoniem voor autorisaties. Het toekennen van autorisaties wordt autoriseren genoemd. Een autorisatie heeft altijd betrekking op *een gebruiker* (een subject) die *een handeling* mag uitvoeren en *een object* waarop of waarmee die handeling wordt uitgevoerd. Voor het uitvoeren van een taak zijn doorgaans vele handelingen op diverse objecten nodig. Om het toekennen van autorisaties te vereenvoudigen wordt een autorisatiestructuur gehanteerd. Handelingen worden gegroepeerd in taken. Taken worden gegroepeerd in rollen. Afhankelijk van door een medewerker uit te voeren werkzaamheden wordt aan het account van de medewerker de benodigde rollen toegekend. In de volgende figuur is dit weergegeven. Het uitwerken van de autorisatiestructuur binnen een ICT-systeem maakt onderdeel uit van het ontwerp van dat ICT-systeem.



Figuur 4: Identity and Accessmanagement

	Toelichting
a	Een gebruiker geeft bij het aanmelden op een systeem de identificatie en de authenticatie kenmerken op van het account waaronder hij of zij wil werken. Een gebruiker heeft doorgaans één account op één ICT-systeem. Omdat meestal op meerdere systemen gewerkt moet worden, resulteert dit in meerdere accounts per gebruiker.
b	De toepassingsbeheerder voert bij de creatie van een account de gebruikersnaam in. Door voor de accounts op de verschillende systemen dezelfde gebruikersnaam te kiezen heeft de gebruiker één gebruikersnaam waaronder hij of zij zich kan aanmelden op de verschillende systemen. De toepassingsbeheerder wordt hierin geholpen door LTB-tooling.
c	Het authenticiteitkenmerk van een account wordt initieel ingevoerd door de toepassingsbeheerder. Bij authenticatie op basis van kennis kan dit kenmerk gewijzigd worden door de gebruiker. Via de servicepunten van Resource Management kan een wachtwoord gereset worden indien een gebruiker zijn wachtwoord vergeten is.
d	De toepassingsbeheerder kent rollen toe aan een account op basis van een aanvraag van de HRM-er van de medewerker.
e	Rollen zijn ontworpen door B/CA SOB team LTB.
f	In de definitiestudie wordt aan de hand van de gewenste functionaliteit van een systeem de taken binnen het systeem ontworpen. Deze taken worden gekoppeld aan rollen.
g	In het basisontwerp wordt ontworpen welke autorisaties nodig zijn om een taak uit te voeren.

De richtlijnen gegeven op hoofdlijnen de volgende uitwerking van Identity and Access Management:

- In IAM R-1 wordt ingegaan op wanneer welke vorm van identificatie en authenticatie gebruikt moet worden;
- IAM R-2 geeft aan hoe het systeem veilig stelt dat een identificatie- en authenticatiemiddel voorbehouden blijft aan de gerechtigde gebruiker;
- IAM R-3 behandelt de fijnmazigheid en de robuustheid van autorisaties;
- in IAM R-4 wordt aangegeven dat verleende toegangsrechten eenvoudig en inzichtelijk moet zijn.

2.1.2 Hoe moet een ICT-systeem gebruikers identificeren en authenticeren?

Richtlijn

IAM R-1	*De toegang tot ICT-systemen is voorbehouden aan bekende identiteiten.*

Risicoafweging

Het gebruik van ICT-systemen is voorbehouden aan bekende personen en processen. Daartoe wordt een registratie bijgehouden van gebruikers (natuurlijke personen én systeemprocessen) en dienen gebruikers zich bekend te maken. Fouten in de registratie of het misleiden van het toegangssysteem kunnen ertoe leiden dat onbevoegden toegang hebben tot de systemen van de Belastingdienst en dat de herleidbaarheid van handelen niet gewaarborgd is.

Norm

IAM N-1-1	Alle gebruikers van ICT-systemen zijn uniek identificeerbaar door één en niet meer dan één gebruikersnaam.

Toelichting

Onder “alle gebruikers van ICT-systemen” wordt verstaan alle personen en alle systeemprocessen die handelingen op systemen uitvoeren. “Uniek identificeerbaar” wil zeggen dat twee gebruikers niet eenzelfde gebruikersnaam mogen hebben. In dat geval zijn namelijk de toegangsrechten niet te koppelen aan unieke gebruikers (zie IAM R-3) en zijn uitgevoerde handelingen niet te herleiden tot natuurlijke personen (zie SM R-1). “Eén en niet meer dan één gebruikersnaam” wil zeggen dat één gebruiker niet twee verschillende gebruikersnamen mag hebben. Anders kunnen namelijk conflicterende handelingen uitgevoerd worden onder verschillende gebruikersnamen, zonder dat waarneembaar is dat de functiescheiding wordt doorbroken (zie IAM N-4-2).

Het systeem is zo ontworpen dat alle gebruikers identificeerbaar zijn door één en niet meer dan één gebruikersnaam. In de exploitatie van het systeem kan besloten worden hiervan af te wijken. Een gebruiker kan voor het uitvoeren van speciale werkzaamheden, zoals beheerwerkzaamheden, een andere gebruikersnaam worden toegekend dan de gebruikersnaam waaronder gewone werkzaamheden worden verricht. Dit valt echter buiten de reikwijdte van het VBI. Het gebruik en beheer van de gebruikersregistratie is namelijk geregeld in het HIB-BBN Belastingdienst. De unieke gebruikersnamen voor het intern domein worden door de toepassingsbeheerder gegenereerd met het LTB-tool (voorheen UUU). Na een werkopdracht van de toepassingsbeheerder wordt een gebruiker opgevoerd door de autorisatiebeheerder van de systeemgerelateerde behandelgroep.

Maatregelen

1. Gebruikers worden binnen ICT-systemen geïdentificeerd door hun unieke gebruikersnaam binnen de Belastingdienst.
2. Vrijgesteld van identificatie zijn gebruikers met toegang tot systemen die alleen toegang kunnen bieden tot publieke informatie. Dit geldt bijvoorbeeld voor de publieke informatie op Internet of beschikbaar gesteld via een informatiekiosk bij de balie. Via een Attack en Penetratietest wordt vastgesteld dat inderdaad alleen tot publieke informatie toegang verkregen kan worden.
3. Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers. Functionele accounts worden aangevraagd bij B/CA SOB team LTB.
4. ICT-systemen bieden de mogelijkheid dat beheerders beheerwerkzaamheden uitvoeren onder hun eigen persoonsgebonden gebruikersnaam. Dit is een eis aan het ICT-systeem dat in het ontwerp wordt meegenomen; in operatie kan besloten worden om beheerwerkzaamheden en werkzaamheden als gewone gebruiker onder twee verschillende, -maar desondanks persoonsgebonden- gebruikersnamen uit te voeren. Het gebruikt van speciale beheer accounts (root, administrator) zijn uitgeschakeld, waarbij uitzonderingen per situatie worden vastgesteld.

Norm

IAM N-1-2	Alvorens een systeem toegang verleent, is de authenticiteit van de gebruiker vastgesteld.

Toelichting

Een gebruiker maakt zich niet alleen bekend, maar de opgegeven identiteit moet ook bewezen worden door het opgeven van een authenticiteitkenmerk. Er zijn verschillende vormen van authenticatie, met oplopende zekerheid dat de gebruiker echt degene is die hij zegt te zijn. De gebruiker kan zijn identiteit bewijzen door kenmerken te geven van iets dat alleen de gebruiker weet (bijvoorbeeld een wachtwoord), bezit (bijvoorbeeld een token), biometrisch karakteriseert (bijvoorbeeld een vingerafdruk), of een combinatie van deze vormen. De sterkte van de toe te passen authenticatie is afhankelijk van gebruik (gewone gebruikers of beheerders), de locatie van waaruit toegang wordt gezocht (binnen of buiten een gebouw van de Belastingdienst) en de zone waarin het doelsysteem staat (externe, e-service, datacenter- of kantoorzone). Niet alle combinaties zijn toegestaan. Een uitleg van de zonering en welke koppelingen tussen zones zijn toegestaan is uitgewerkt in het onderdeel Boundary Protection (zie paragraaf 2.5).

Maatregelen

1. Gebruikers van poortsystemen (dat zijn relaties van de Belastingdienst) authenticeren zich indien er persoongebonden informatie wordt uitgewisseld. Authenticatie vindt bij voorkeur plaats op basis van DigiD.
2. Bij het intern gebruik van ICT-systemen (door eigen medewerkers van de Belastingdienst of inhuurde medewerkers) worden gebruikers minimaal geautenticeerd op basis van wachtwoorden.
3. Authenticatie van gebruikers vindt naast op basis van wachtwoorden (zie IAM N-1-2 1) bovendien plaats op basis van een One Time Password token (momenteel van het merk RSA SecurID) met een pincode indien:
   a. met ICT-systemen wordt gewerkt met overwegend bijzonder vertrouwelijke informatie (een systeem in een extra afgeschermd compartiment binnen de data center zone, zie BP N-2-1);
   b. vanuit een externe locatie wordt gewerkt (buiten een gebouw van de Belastingdienst);
   c. kritische beveiligingscomponenten worden beheerd (denk bijvoorbeeld aan Hardware Security Modules, firewals, Intruder detection en routers).
4. Bij het beheer van kritische beveiligingscomponenten wordt een vierhanden principe toegepast (dat wil zeggen dat er altijd twee functionarissen nodig zijn om een handeling uit te voeren).
5. Een mobiel apparaat (zoals een handheld computer, Smartphone, PDA) moet de mogelijkheid bieden om een pincode of wachtwoord te vragen bij het inschakelen van het apparaat.
6. Bij telewerken, beheer op afstand en mobiel werken (een mobiel apparaat dat radiografisch verbonden is met ICT-systemen van de Belastingdienst) wordt vastgesteld dat vanaf een voor dit doeleinde beschikbaar gestelde werkplek wordt gewerkt.
7. Functionele accounts (accounts van systeemprocessen) vereisen in een aantal gevallen geen authenticatie. Dit wordt beoordeeld door een beveiligingsarchitect. Overweging daarbij is onder meer dat het gebruik geheel automatisch verloopt en interactief gebruik van het account technisch onmogelijk is.

Richtlijn

IAM R-2	*De exclusiviteit van het identificatie- en authenticatiemiddel moet gewaarborgd zijn.*

Risicoafweging

Wanneer iemand de beschikking heeft over het identificatie- en authenticatiemiddel van iemand anders, dan kan diegene daarmee toegang tot gegevens en functionaliteit krijgen die voorbehouden zijn aan anderen.
Er zijn veel aanvallen waarmee gebruikersnamen en wachtwoorden te achterhalen zijn. De normen onder deze richtlijn gaan over het afdwingen van sterke wachtwoorden (IAM N-2-1) en het configureren van de aanmelding op systemen (IAM N-2-2), zodat misbruik zoveel mogelijk wordt tegengegaan.

Binnen andere aandachtsgebieden en andere handboeken worden maatregelen genomen om de andere aanvallen te pareren. Enkele voorbeelden:

- Wachtwoorden worden versleuteld opgeslagen en gecommuniceerd (zie VBI ENC N-1-2)
- Het afvangen van ingetoetste wachtwoorden met behulp van keystroke loggers wordt voorkomen door alleen gecertificeerde apparatuur en programmatuur toe te laten in de productie en acceptatieomgeving (zie HIB CICT Ex N-1-1 en VBI SM N-3-1).
- Het doorgeven van wachtwoorden door gebruikers aan andere gebruikers is technisch niet te voorkomen. Het is de verantwoordelijk van het management van een Belastingdienstkantoor gebruikers er op te wijzen dat wachtwoorden strikt geheim gehouden moeten worden (zie HIB-BBN 2005 P&O N-4-2).

Norm

IAM N-2-1	Het systeem dwingt het gebruik van sterke wachtwoorden af.

Toelichting

In de meeste systemen is het wachtwoord de belangrijkste barrière om te voorkomen dat iemand werkt onder een andere dan de eigen gebruikersnaam. Het risico bij het doorbreken van deze barrière is dat handelingen verricht worden waarvoor iemand niet geautoriseerd is en dat handelingen niet terug te voeren zijn tot degene die deze handelingen heeft uitgevoerd. Daarom moeten wachtwoorden zo gekozen worden dat ze moeilijk te raden zijn (sterke wachtwoorden) en dat afgedwongen wordt dat wachtwoorden geregeld worden gewijzigd. Hierbij wordt naar het optimum in veiligheid en toch eenvoudig te onthouden wachtwoorden gezocht. De ervaring leert dat naarmate wachtwoorden moeilijker te onthouden zijn, de wachtwoorden worden opgeschreven door de gebruikers, waardoor anderen hier kennis van zouden kunnen nemen. Met name de veelheid aan verschillende wachtwoorden werkt het opschrijven in de hand.

Maatregelen

1. Wachtwoorden voldoen aan de volgende wachtwoordconventie:
   a. Wachtwoorden zijn minimaal 8 tekens lang;
   b. een teken in een wachtwoord komt niet vaker dan twee maal voor;
   c. een wachtwoord bevat ten minste één letter, één cijfer en één speciaal teken;
   d. het wachtwoord verschilt in minimaal 3 tekens van het vorige wachtwoord;
   e. het wachtwoord is niet gelijk aan de laatste 5 gebruikte wachtwoorden
2. Wachtwoorden van gebruikersaccounts moeten minimaal elke 90 dagen gewijzigd worden.
3. Wachtwoorden van functionele accounts worden minder frequent gewijzigd, namelijk minimaal ééns per jaar en ten minste elke nieuwe release van de ICT service, maar daarentegen zijn de wachtwoorden langer, namelijk minimaal 20 posities, met willekeurig gekozen cijfers, tekens en speciale tekens.
4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
   a. Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd;
   b. ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure;
   c. alvorens een nieuw wachtwoord wordt gewijzigd, wordt geautomatiseerd gecontroleerd of het nieuwe wachtwoord aan de vereiste conventie voldoet.
5. De default en installatiewachtwoorden worden tijdens of direct na installatie verwijderd of gewijzigd.
6. Initiële wachtwoorden en wachtwoorden die gereset zijn, voldoen aan bovenstaande wachtwoordconventie en daarbij wordt door het systeem afgedwongen dat bij het eerste gebruik dit wachtwoord wordt gewijzigd.

Norm

IAM N-2-2	Instellingen met betrekking tot het aanmelden op een systeem zijn er op gericht te voorkomen dat iemand werkt onder een andere dan de eigen gebruikersnaam.

Toelichting

Ondanks dat gebruikers sterke wachtwoorden kiezen (zie IAM N-2-1) blijft het risico bestaan dat personen onder iemands anders account werken en daarmee de bevoegdheden van dat account kunnen misbruiken. ICT-systemen dienen daarom zo geconfigureerd te worden dat dit zoveel mogelijk voorkomen wordt.

Maatregelen

1. Er wordt zoveel mogelijk voorkomen dat gebruikers zich op verschillende systemen opnieuw aan moeten melden (er wordt gestreefd naar reduced sign on, waarbij een gebruiker voor verschillende systemen zoveel mogelijk één security context heeft). Indien dit niet mogelijk is dan dient het aanmeldproces zo veel mogelijk enkelvoudig te worden ingericht (zie ook IAM N-4-3).
2. Accounts moeten voorzien kunnen worden van een expiratiedatum.
3. Op het eindgebruikers platform wordt gebruik gemaakt van schermbeveiligingsprogrammatuur (een screensaver) die na 30 minuten alle informatie op het beeldscherm onleesbaar maakt. Het is toegestaan dat het systeem zo geconfigureerd wordt, dat binnen een grace period van enkele seconden de gebruiker door een muisbeweging of toetsenbordaanslag kan verhinderen dat de schermbeveiliging wordt geactiveerd. Het systeem biedt de gebruiker ook zelf de mogelijkheid om de schermbeveiliging op eenvoudige wijze te activeren. Het systeem is zo ingesteld dat na het activeren van de schermbeveiliging de gebruiker zich opnieuw moet authenticeren (de identificatie mag zichtbaar blijven).
4. Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden dan wordt het account geblokkeerd, totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.
5. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven van het wachtwoord. Het is wel gebruikelijk dat toetsaanslagen worden weergegeven door sterretjes of bullets.
6. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
7. Voordat een geslaagde aanmelding op een systeem heeft plaatsgevonden toont het systeem uitsluitend informatie die noodzakelijk is voor de aanmelding. Er wordt dus geen informatie getoond over servers, netwerken, gebruikersnamen en dergelijke. Bij een foutieve aanmelding wordt niet vermeld of de gebruikersnaam bestaat, maar slechts dat de combinatie gebruikersnaam en wachtwoord onjuist was. Er wordt bovendien geen geheugensteun voor het wachtwoord getoond (mogelijkheid in Windows XP).
8. Automatisch aanmelden is niet toegestaan voor interactieve gebruikers. Hier wordt bedoeld dat automatisch wordt ingelogd zonder dat binnen de sessie door een gebruiker een wachtwoord wordt ingegeven (bijvoorbeeld het gebruik van Windows Auto Log-on mag dus niet, waarbij door het aanzetten van een PC een gebruiker automatisch wordt ingelogd onder een vooraf opgegeven gebruikersnaam met een vooraf opgegeven wachtwoord). Alleen systeemprocessen met functionele accounts mogen geautomatiseerd aanloggen. Single Sign On is ook toegestaan, mits andere normen worden nageleefd (zie bijvoorbeeld het gebruik van sterke wachtwoorden zie IAM N-2-1 en het encrypt communiceren en opslaan van wachtwoorden ENC N-1-2).

2.1.3 Hoe moet een ICT-systeem gebruikers toegang verlenen?

Richtlijn

IAM R-3	*De toegang tot ICT-systemen is beperkt tot geautoriseerde gebruikers.*

Risicoafweging

Het risico bestaat dat onbevoegde personen (opzettelijk of onopzettelijk) gegevens van de Belastingdienst kunnen raadplegen of wijzigen. Hierdoor kan de integriteit en de vertrouwelijkheid van gegevens geschonden worden. Daarbij bestaat tevens het risico dat de beschikbaarheid van ICT-systemen in gevaar wordt gebracht. Het hanteren van een systeem voor logische toegangsbeveiliging is de verantwoordelijkheid van het management van de Belastingdienstkantoren (zie HIB-BBN 2005 in INF R-2). Het management van de Belastingdienstkantoren bepaald dus wie geautoriseerde gebruikers zijn.

Een constructie voor logische toegangsbeveiliging beperkt de toegang tot deze geautoriseerde gebruikers, waarbij:

- de toegang wordt beperkt tot uitsluitend dat wat toegestaan is (IAM N-3-1);
- onbedoeld gebruik van autorisaties wordt beperkt (IAM N-3-2);
- handelingen met minimale toegangsrechten worden uitgevoerd (IAM N-3-3).

Norm

IAM N-3-1	Op alle objecten moet toegangsbeveiliging van toepassing zijn op basis van: “Niets mag, tenzij dit is toegestaan”.

Toelichting

De tegenhanger “Alles mag, tenzij dit wordt verboden” is minder veilig. Een vergeten aan te brengen restrictie leidt dan namelijk tot toegang tot het systeem. “Niets mag, tenzij dit is toegestaan” betekent dat er wordt nagegaan welke autorisaties een medewerker nodig heeft en dat de medewerker niet meer autorisaties krijgt dan strikt noodzakelijk. Een vergeten toe te kennen permissie leidt daarmee nooit tot ongewenste toegang. De manier waarop autorisaties aan medewerkers worden gekoppeld, is uitgewerkt in IAM R-4.

Maatregelen

1. In de soort permissies wordt ten minste onderscheid gemaakt tussen lees- en schrijfpermissies. De mogelijkheden om permissies fijnmazig toe te kennen is afhankelijk van het object. Algemeen geldt hoe fijnmaziger hoe beter en als het systeem de mogelijkheid biedt dan moet het gebruikt worden. Zo kunnen bij schrijfrechten vaak rechten voor creëren (zoals create/insert/generate), wijzigen (zoals update/change/alter) en verwijderen (zoals delete/drop/purge) separaat worden toegekend.
2. Toegangsbeveiliging is geïmplementeerd op alle objecten die gegevens bevatten of verwerken. Dit betreft onder meer de volgende objecten:
   a. Platforms (PC, PPC, server, mainframe, mobiele werkplek): bestanden, directories, services en randapparatuur (denk aan USB devices op de werkplek);
   b. Netwerken: Toegangsbeveiliging van netwerksegmenten kan met de huidige netwerkinfrastructuur niet worden ingericht op gebruikersniveau, maar vindt plaats op basis van het IP-nummer van het werkstation. Daarom wordt dit niet verder bij IAM uitgewerkt maar bij Boundary Protection (zie BP N-2-2);
   c. Ondersteunende systemen: services;
   d. Primaire systemen: taken/functies in applicaties, methods, stored procedures, gegevensbenadering in databases (views, tabellen, velden, records);
   e. Bedrijfsvoering: taken/functies in pakketten, gegevensbenadering in databases (views, tabellen, velden, records);
   f. Beheer: Beheer van appliances en firmware van hardware voor zover dit kan. Mogelijk is er geen functionaliteit op de toegang tot firmware met een rechtenstructuur te beveiligen. Wel dient in ieder geval een wachtwoord te zijn ingesteld.

Norm

IAM N-3-2	Er zijn maatregelen getroffen die onbedoeld gebruik van toegekende autorisaties voorkomen.

Toelichting

Autorisaties worden toegekend om handelingen onder bepaalde voorwaarden mogelijk te maken. Handelingen buiten deze gebruiksvoorwaarden om worden zoveel mogelijk door technische maatregelen geblokkeerd.

Maatregelen

1. Gebruikers krijgen geen algemene commando-omgeving tot hun beschikking (bijvoorbeeld een dos-prompt of unix-shell.
2. Beheertaken verlopen zoveel mogelijk via een menusysteem en gestandaardiseerde werkwijzen (scripts).
3. Bij het overnemen van werkstations door beheerders om te kunnen meekijken op het werkstation wordt technisch afgedwongen dat hiervoor eerst toestemming aan de gebruiker wordt gevraagd. De gebruiker kan op elk moment de verleende toestemming intrekken.
4. Systeemdata, programmatuur en toepassingsgegevens zijn van elkaar gescheiden, dat wil zeggen dat de bestanden zoveel mogelijk in eigen directories of partities geplaatst worden.
5. Er worden geen hulpmiddelen gebruikt die het systeem van logische toegangsbeveiliging doorbreken (denk aan ODBC, bestandsviewers en editors waarmee bestanden rechtstreeks gewijzigd kunnen worden in plaats van dat dit alleen kan via een applicatie die controleert of de benodigde toegangsrechten aanwezig zijn).
6. Besturingsprogrammatuur heeft de mogelijkheid zowel programma-, netwerk- als gebruikerssessies af te sluiten.
7. Er wordt tijdens het ontwerp van een systeem expliciet uitgewerkt of gebruik gelimiteerd kan worden tot een bepaalde tijdshorizon. Buiten deze tijdshorizon kan er dan geen gebruik (en dus ook geen misbruik) van het systeem gemaakt worden. Denk bijvoorbeeld aan beperking van de mogelijkheid om aan te melden bij systemen buiten kantooruren, beperking van de maximale verbindingstijd en het just-in-time klaar zetten van bestanden voor filetransfer en toegang voor onderhoud op afstand door een leverancier alleen openstellen op basis een wijzigingsverzoek of storingsmelding.

Norm

IAM N-3-3	Handelingen worden uitgevoerd met zo weinig mogelijk rechten.

Toelichting

Dit beveiligingsprincipe staat bekend als “least privileged principle”. Door handelingen uit te voeren met zo weinig mogelijk rechten, wordt voorkomen dat onnodige vrijheden in toegangsrechten worden gebruikt of beter gezegd worden misbruikt. Schade die kan ontstaan (bijvoorbeeld bij systeemfouten) wordt daardoor beperkt.

Maatregelen

1. De toekenning van rechten aan processen is zo minimaal mogelijk. Bijvoorbeeld:
   a. Als het platform toestaat om gescheiden executie- en leesrechten toe te kennen, dan worden voor programmabestanden geen leesrechten toegekend.
   b. Tijdelijke (spool)bestanden (bijv. printgegevens) zijn niet voor onbevoegden toegankelijk.
2. Toepassingen mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn wordt weer terug geschakeld naar het niveau van een gewone gebruiker (een unprivileged user). Denk bijvoorbeeld aan een daemon die onder root een poort opent en daarna terugschakelt naar userniveau. Ander voorbeeld is het gebruik het Subsitute User commando. Dit wordt alleen gebruikt voor die delen van een proces die tijdelijk onder hogere rechten draaien.
3. De taken die met (tijdelijk) hogere rechten uitgevoerd worden, kunnen niet onderbroken of afgebroken worden met als gevolg dat deze hogere rechten voor andere doeleinden gebruikt kunnen worden (feitelijk misbruikt kunnen worden).

Richtlijn

IAM R-4	*Verleende toegangsrechten zijn inzichtelijk en beheersbaar.*

Risicoafweging

Een eenvoudige en inzichtelijke structuur maakt het beheer van toegangsrechten eenvoudiger en verminderd de kans op fouten. De verleende toegangsrechten moeten altijd overeenstemmen met de aangevraagde toegangsrechten, om onbedoeld gebruik van een systeem te voorkomen. Het is de verantwoordelijkheid van het lijnmanagement van een Belastingdienstkantoor dat er een administratie wordt gevoerd waaruit blijkt dat de goedgekeurde en de in de systemen aanwezige toegangsrechten overeenstemmen (zie HIB-BBN 2005 INF N-2-2). Uit de ICT-systemen moeten daartoe de gestructureerde en actueel verleende rechten opgevraagd kunnen worden. In termen van normen betekend dit dat:

- de rechtenstructuur eenduidig gestructureerd is (IAM N-4-1);
- er rekening gehouden is met functiescheiding en need-to-know (IAM N-4-2);
- single-point-of-administration wordt nagestreefd (IAM N-4-3);
- de verleende rechten inzichtelijk zijn (IAM N-4-4).

Norm

IAM N-4-1	Toegangsrechten worden toegekend op basis van een stelsel van rollen en taken (Role Based Access Control).

Toelichting

Rollen en taken zijn een verzameling aan elkaar gerelateerde autorisaties. Deze toegangsrechten worden gegroepeerd om het beheer (het toekennen, onderhouden en intrekken) van rechten te vereenvoudigen. Toegangsrechten op de onderliggende objecten zijn dermate massaal dat de beheerbaarheid zonder goede structuur problematisch is en er snel fouten in de toekenning gemaakt kunnen worden.

Maatregelen

1. In het ontwerp wordt de rechtenstructuur gestructureerd volgens een stelsel van rollen en taken, waarbij:
   a. rollen zoveel mogelijk aansluiten op het standaard Role Based Access Control model, zoals dat is ontwikkeld door Team Logisch ToegangsBeheer van B/CA SOB;
   b. de taken en de koppeling van taken aan rollen wordt uitgewerkt in de definitiestudie;
   c. de benodigde autorisaties voor het uitvoeren van taken wordt uitgewerkt in het basisontwerp.
2. Indien afgeweken wordt van het standaard Role Based Access Control model voorziet het ontwerp in de mogelijkheid om via een groeperingmechanisme toegangsrechten aan gebruikers toe te kennen (dus niet rechtstreeks aan individuele gebruikers).
3. Voor rollen en taken geldt een naamgevingconventie.

Norm

IAM N-4-2	Toegangsrechten worden toegekend op basis van het “need-to-know”-beginsel en zijn conform de functiescheiding binnen de organisatie

Toelichting

“Need-to-know” wil zeggen dat een gebruiker alleen die rechten krijgt, die hij daadwerkelijk nodig heeft voor het uitoefenen van de functie. Dit kan door fijnmazig toegangsrechten op individuele basis toe te kennen aan gebruikers, maar dat leidt tot een onbeheersbare autorisatiestructuur. Daarom wordt gebruik gemaakt van rollen en taken (zie ook IAM N-4-1). De ontworpen rollen en taken moeten aansluiten op de functies die onderkend worden binnen een Belastingdienstkantoor.

Wanneer dit niet goed aansluit kan de situatie ontstaan dat aan een medewerker te veel rechten toegekend moeten worden om zijn functie uit te kunnen voeren. Dit kan bijvoorbeeld ontstaan indien een medewerker raadpleegbevoegdheid op een object nodig heeft en deze bevoegdheid alleen in een beheerdersrol is opgenomen.

Maatregelen

1. Aan rollen en taken worden uitsluitend toegangsrechten gekoppeld die absoluut nodig zijn om een taak uit te voeren.
2. Er worden geen, of anders zo weinig mogelijk rechten gegeven aan algemene groepen als “guest”, “public” of “everyone”.
3. Een rol bevat nooit een zodanige set van autorisaties dat dit de functiescheiding doorbreekt.
4. Het systeem wordt zo ontworpen dat beheerrollen nooit aan gewone gebruikers toegekend hoeven worden, maar uitsluitend aan beheerders.
5. Beheertaken worden uitsluitend aan een beheerrol gekoppeld.
6. Vergaande autorisaties (beheerrechten of privileged rights) worden uitsluitend aan beheertaken gekoppeld.

Norm

IAM N-4-3	De verleende toegangsrechten worden zoveel mogelijk enkelvoudig geadministreerd (single-point-of-administration).

Toelichting

Meerdere voorkomens van toegangsrechtenregistraties werkt verschillen tussen deze registraties en fouten in de verleende toegangsrechten in de hand.

Maatregelen

1. De administratie van gebruikers en verleende toegangsrechten is zoveel mogelijk centraal geregeld (denk aan: centrale authenticatie, TP-monitoren, DBMS-en, beheer- en beveiligingstools). Hierbij wordt zoveel mogelijk aangesloten op bestaande administraties:
   a. Mainframe – RACF;
   b. Midrange – Kerberos;
   c. PC Clients/Servers – Active Directory ;
   d. Netwerk componenten – Radius (Radius is niet perse een separate registratie maar is bij voorkeur geïntegreerd met Active Directory);
   e. e-Service zone – Afsprakenadministratie.
2. De validatie van toegangsrechten (autorisation decision) wordt zoveel mogelijk door generieke permissie infrastructuur afgehandeld (er zijn hiervoor momenteel meerdere autorisatie-voorzieningen operationeel, bijvoorbeeld BEA en AUT. Op welke voorziening wordt aangesloten maakt niet zo veel uit, zolang er maar geen nieuwe autorisatievoorziening wordt ontworpen).

Norm

IAM N-4-4	Op elk moment moet het inzichtelijk zijn over welke actuele totale set van rechten een gebruiker beschikt.

Toelichting

Voor controle doeleinden moet uit de ICT-systemen de verleende rechten opgevraagd kunnen worden. Onder meer is dit nodig om vast te kunnen stellen dat de goedgekeurde toegangsrechten overeenstemmen met de in de ICT-systemen aanwezige toegangsrechten.

Maatregelen

1. Er wordt centraal geregistreerd wie welke totaal set van autorisaties heeft binnen de Belastingdienst. Hierbij worden onderkend:
   a. Systeem autorisaties;
   b. Applicatie/Taak autorisaties;
   c. Gegevens autorisaties.
2. Het is voor beheerders mogelijk de toegangsrechten op te vragen die gekoppeld zijn aan:
   a. accounts;
   b. rollen;
   c. taken.

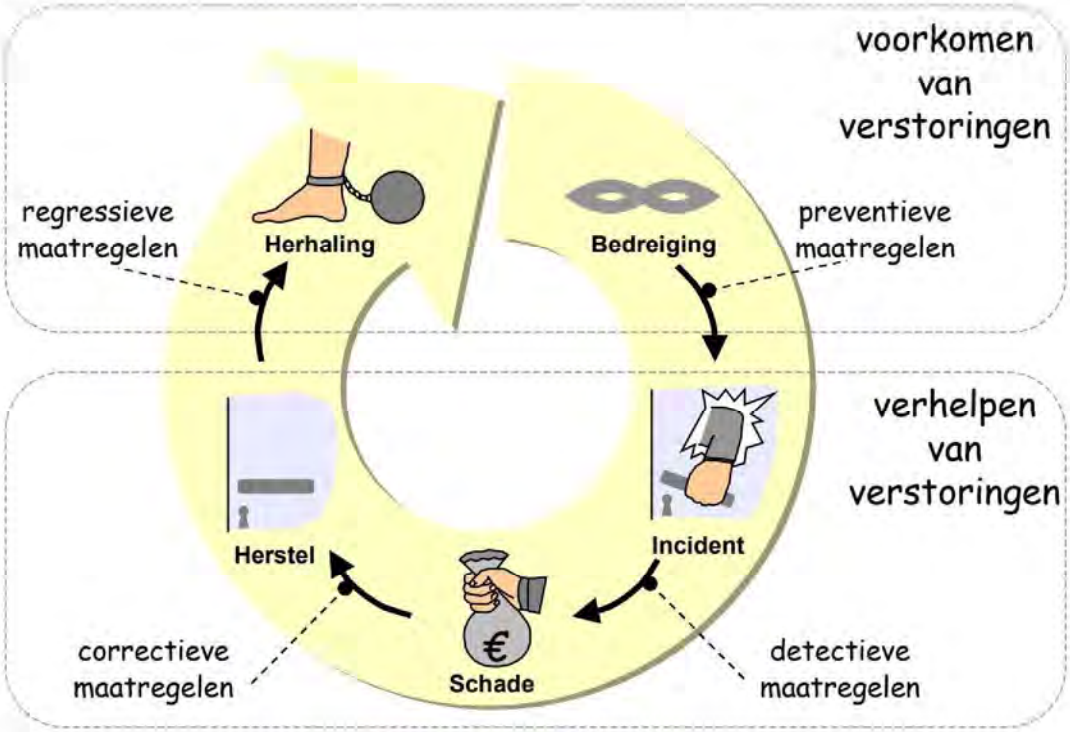
3. Het is voor de beheerders mogelijk op te vragen:
   a. wie de eigenaar van een account is, dat wil zeggen welke medewerker welke gebruikersnaam heeft of bij functionele accounts wie de functionele eigenaar is;
   b. welke totale set autorisaties een gebruikers heeft;
   c. welke gebruikers bepaalde toegangsrechten hebben;
   d. aan welke gebruikers een combinatie van toegangsrechten zijn toegekend die uit oogpunt van functiescheiding onverenigbaar zijn.

2.2 Security Monitoring

2.2.1 Wat is security monitoring?

Dectectieve maatregelen

Security monitoring is het treffen van detectieve beveiligingsmaatregelen om vast te stellen of de beveiliging van de organisatie aantoonbaar effectief is. Detectieve maatregelen zijn maatregelen gericht op het tijdig detecteren van beveiligingsincidenten en zwaktes in de beveiliging.



Figuur 5: Security monitoring is het treffen van detectieve beveiligingsmaatregelen

Beveiligingsincidenten zijn nooit helemaal te voorkomen, hoe goed de preventieve maatregelen ook zijn. Het is bovendien niet de bedoeling te streven naar waterdichte beveiliging; dit zou veel te kostbaar zijn. Daarentegen wordt getreeft naar acceptabele restrisico's. Security Monitoring geeft inzicht in het restrisico's dat daadwerkelijk optreedt of opgetreden is. Zonodig kunnen vervolgens correctieve en regressieve maatregelen genomen worden.

Een goed voorbeeld dat er altijd restrisico's bestaan is dat ondanks strenge test- en acceptatieprocedures er eigenlijk altijd nog fouten in ICT-systemen zitten. Sommige van die fouten kunnen worden uitgebuit om de beveiliging te doorbreken. Leveranciers brengen vaak updates uit, ook wel patches genoemd, om die fouten te repareren. Bij apparatuur vindt een update vaak plaats in de vorm van een driver of firmware update. Zwakheden in de beveiliging kunnen ook ontstaan door het onjuist configureren van een ICT-systeem. Vaak is dat initieel niet bekend en blijkt pas in de loop der tijd dat een bepaalde configuratie zwak is. Geautomatiseerde hulpmiddelen ondersteunen het dectecteren van zwakheden.