Algemene Rekenkamer

Rijksbreed bedrijfsvoeringsonderzoek in het kader van het verantwoordingsonderzoek 2011 - Achtergronddocument

Informatiebeveiliging en vertrouwensfuncties

16 mei 2012

Algemene Rekenkamer
Lange Voorhout 8
Postbus 20015
2500 EA Den Haag

070 - 3424344
voorlichting@rekenkamer.nl
www.rekenkamer.nl

Inhoud

1 Over dit onderzoek

Gelet op het belang van informatiebeveiliging voor het presteren en functioneren van de rijksdienst hebben we daar binnen het verantwoordingsonderzoek 2011 bij alle ministeries onderzoek naar gedaan. Uitval van computers, het zoek raken van bestanden of het door onbevoegden kennis nemen van informatie – om maar een paar voorbeelden te noemen – kan ernstige gevolgen hebben voor burgers, bedrijven en overheden. De samenleving moet erop kunnen vertrouwen dat (overheids-)organisaties zorgvuldig omgaan met informatie.

Bij alle ministeries en bij één baten-lastendienst van elk ministerie[1] hebben we onderzoek gedaan naar:

- de kwaliteit van het informatiebeveiligingsbeleid;
- de bescherming van informatiesystemen.

Daarnaast hebben we bij alle ministeries onderzoek gedaan naar vertrouwensfuncties, zowel naar het aanwijzen van een functie als vertrouwensfunctie als naar het uitvoeren van veiligheidsonderzoeken naar de personen die die functies vervullen.

In ons rapport *Staat van de rijksverantwoording 2011*[2] concluderen we dat de meeste ministeries niet de noodzakelijke aandacht geven aan informatiebeveiliging. We hebben in totaal negen onvolkomenheden geconstateerd bij vijf ministeries.[3]

---

[1] De Ministeries van Algemene Zaken, Buitenlandse Zaken en Financiën beschikken niet over baten-lastendiensten met gevoelige informatie. Om deze reden is bij deze ministeries geen baten-lastendienst onderzocht. Bij het Ministerie van Financiën hebben wij naast het kernministerie in plaats van een baten-lastendienst de Belastingdienst onderzocht, omdat dit een maatschappelijk vitale dienst is, waarbij de informatiebeveiliging van groot belang is. Bij het Ministerie van Volksgezondheid, Welzijn en Sport hebben wij twee baten-lastendiensten onderzocht (College ter Beoordeling van Geneesmiddelen en Rijkinstituut voor Volksgezondheid en Milieu) vanwege de daar geconstateerde onvolkomenheden in ons verantwoordingsonderzoek over 2010.

[2] Algemene Rekenkamer (2012). *Staat van de rijksverantwoording 2011.* Tweede Kamer, vergaderjaar 2011-2012, xx xxx, nrs x en x. Den Haag: Sdu.

[3] Bij de Belastingdienst (Ministerie van Financiën) is extra onderzoek verricht naar de logische toegangsbeveiliging, hetgeen in combinatie met de resultaten van het rijksbrede onderzoek naar informatiebeveiliging leidde tot een onvolkomenheid op informatiebeveiliging naast de vermelde negen.

Ook voor de vertrouwensfuncties moet meer aandacht komen: slechts een deel van de onderzochte ministeries en baten-lastendiensten beschikt over een sluitende administratie en bij veel ministeries en diensten zijn medewerkers werkzaam in een vertrouwensfunctie zonder dat zij zijn gescreend. We hebben twee onvolkomenheden geconstateerd: de Belastingdienst heeft een sterk verouderd overzicht van vertrouwensfuncties en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft grote achterstanden in het uitvoeren van de veiligheidsonderzoeken (herhaalonderzoeken) voor het Ministerie van Defensie.
Over de onvolkomenheden rapporteren we in de betreffende rapporten bij de jaarverslagen. Deze rijksbrede rapportage heeft tot doel om ministeries en baten-lastendiensten te stimuleren om hun informatiebeveiliging en het beheer van de vertrouwensfuncties te verbeteren. We laten niet alleen zien *dat* er wat te verbeteren valt, maar aan de hand van enkele goede voorbeelden, ook *hoe*.

Methodologie
Voor het onderzoek naar informatiebeveiliging en vertrouwensfuncties hebben wij het beleid en de praktijk getoetst aan de van toepassing zijnde wet- en regelgeving[4]. Hiervoor hebben wij op basis van deze wet- en regelgeving een vragenlijst ontwikkeld (zie bijlage 1). Ook voor de gangbare maatregelen van toegangsbeveiliging van informatiesystemen (bijvoorbeeld wachtwoorden en controles op computervirussen) hebben wij een vragenlijst ontwikkeld, die wij hebben gebaseerd op vakliteratuur[5] (zie bijlage 2).

[4] De toepasselijke wet- en regelgeving bestaat uit de Wet veiligheidsonderzoeken, de Wet bescherming persoonsgegevens, het Beveiligingsvoorschrift Rijksdienst 2005, het Besluit voorschrift informatiebeveiliging rijksdienst 2007 en het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie. De Wet bescherming persoonsgegevens hebben wij in ons onderzoek buiten beschouwing gelaten, omdat het CBP al toezicht houdt op de naleving daarvan.
[5] Bij deze vragenlijst hebben wij ons onder meer gebaseerd op de Code voor Informatiebeveiliging en Cobit.

2 Kwaliteit informatiebeveiligingsbeleid

Wij hebben de kwaliteit van het informatiebeveiligingsbeleid beoordeeld op basis van de relevante regelgeving:

- het Beveiligingsvoorschrift Rijksdienst 2005;
- het Besluit voorschrift informatiebeveiliging rijksdienst (VIR) 2007;
- het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (VIR-BI).

Op grond van deze regelgeving moet het informatiebeveiligingsbeleid minimaal aan tien eisen voldoen. Wij zijn voor alle ministeries en voor de onderzochte baten-lastendiensten per eis nagegaan in welke mate ze eraan voldoen. In bijlage 3 staat wat die eisen zijn en hoe de verschillende departementen daar op scoren.[6]

De meeste ministeries en baten-lastendiensten scoren slecht op de volgende twee punten:

- Niet voor alle informatiesystemen en informatieketens[7] is duidelijk wie hiervoor verantwoordelijk is.
- Een periodieke evaluatie van het informatiebeveiligingsbeleid is niet gepland of wordt niet uitgevoerd.

Vooral de verantwoordelijkheid voor informatieketens is veelal niet duidelijk. Als niet duidelijk is wie voor welk systeem binnen de keten verantwoordelijk is, kunnen geen afspraken worden gemaakt over de beveiliging van die systemen en bestaat het risico dat het gewenste beveiligingsniveau van de keten niet wordt gerealiseerd.
Bij ons onderzoek hebben wij geconstateerd dat het toewijzen van verantwoordelijkheden voor ketens wel op orde is bij de Ministeries van Buitenlandse Zaken (BuZa), Defensie, Financiën (Belastingdienst), Sociale Zaken en Werkgelegenheid (SZW), Veiligheid en Justitie (VenJ) en bij de

[6] In bijlage 5 staat een grafiek waarin de scores voor zowel beveiligingsbeleid als bescherming van systemen gewogen bij elkaar zijn opgeteld.

[7] Ketens van onderling afhankelijke informatiesystemen.

baten-lastendiensten IVENT[8] (Defensie), DICTU[9] (Economische Zaken, Landbouw en Innovatie –EL&I) – zie kader –, Rijkswaterstaat (Infrastructuur en Milieu – IenM), Agentschap SZW en het Centraal Justitieel Incasso Bureau (VenJ).

Goed praktijkvoorbeeld informatieketens: DICTU van het Ministerie van EL&I

DICTU administreert alle informatiesystemen die worden beheerd in het informatiesysteem Applicatie Portfolio Management systeem (APM). In APM wordt aangegeven welke lijnmanager eigenaar is van welk informatiesysteem. DICTU geeft aan dat het team Ketenmanagement operationeel verantwoordelijk is voor 16 kritische informatieketens.

In het informatiebeveiligingsbeleid van bijna alle ministeries en baten-lastendiensten staat dat periodiek een evaluatie moet plaatsvinden. Bij veel ministeries en baten-lastendiensten wordt een dergelijke evaluatie echter niet of niet tijdig uitgevoerd. Hierdoor laten ministeries en baten-lastendiensten kansen onbenut om het informatiebeveiligingsbeleid te verbeteren. Ook ontstaan hierdoor mogelijk risico's voor de bedrijfs- en beleidsvoering, omdat het informatiebeveiligingsbeleid niet wordt aangepast op basis van organisatieontwikkelingen en beveiligingsincidenten. Ministeries en diensten die het informatiebeveiligingsbeleid wel periodiek evalueren zijn: Algemene Zaken (AZ) – zie kader –, BuZa, Defensie, IVENT (Defensie), DICTU (EL&I), Financiën, Belastingdienst.

Goed praktijkvoorbeeld evaluatie informatiebeveiligingsbeleid: Ministerie van AZ

In hoofdstuk 11 van het Beleidsdocument Informatiebeveiliging (IB) van het Ministerie van AZ wordt beschreven dat er gebruik wordt gemaakt van de kwaliteitscirkel van Deming[10]. Onderdeel hiervan is een evaluatie van de resultaten vanuit de audits en de periodieke controlewerkzaamheden. In het Beleidsdocument IB wordt ook beschreven dat de centrale Informatiebeveiligingsfunctionaris tweejaarlijks het informatiebeveiligingsbeleid evalueert. Het departement geeft aan dat het naar aanleiding van recente ontwikkelingen, zoals een interne reorganisatie en het gebruik van het tactisch normenkader Digitale Werkomgeving Rijksdienst (DWR), het huidige informatiebeveiligings-beleid hebben geëvalueerd; als gevolg hiervan wordt het informatiebeveiligingsbeleid geactualiseerd.

[8] De bedrijfsgroep Informatievoorziening en -Technologie (IVENT) van Defensie levert diensten op het gebied van informatievoorziening (IV), ICT en documentaire informatie.

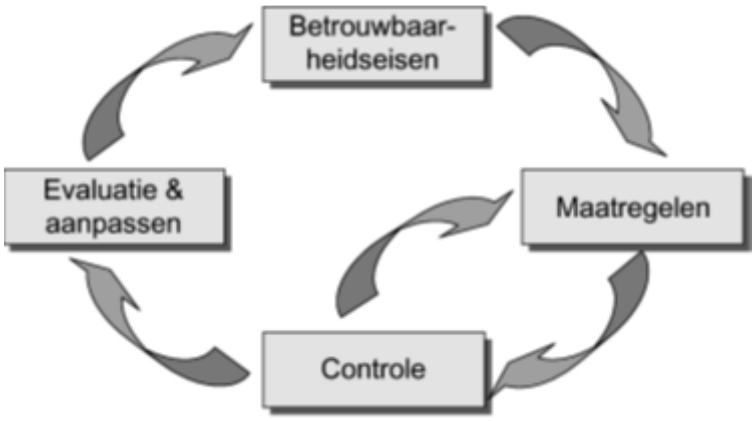
[9] DICTU is Dienst ICT Uitvoering.

[10] Dit is de Plan Do Check Act cyclus. Zie ook figuur 1 op pagina 5.

3 Bescherming van informatiesystemen

Het informatiebeveiligingsbeleid moet in de praktijk leiden tot bescherming van informatiesystemen. Het uiteindelijke doel is om voor elk informatiesysteem een samenhangend pakket van beveiligingsmaatregelen te treffen om de risico's van inbraak, misbruik en uitval van informatiesystemen[11] te beheersen. Het lijnmanagement[12] is op de werkvloer verantwoordelijk voor de beveiliging van informatiesystemen voor de aan hen toevertrouwde bedrijfsprocessen. In het VIR 2007 is de gewenste aandacht van het management voor informatiebeveiliging ingebouwd door Informatiebeveiliging te benaderen via de kwaliteitscirkel van Deming (Plan Do Check Act-cyclus – PDCA cyclus, zie figuur 1).

Figuur 1 PDCA cyclus voor informatiebeveiliging



[11] Informatiesysteem: een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie (artikel 1, lid b, VIR 2007).

[12] Het begrip lijnmanagement wordt hierbij ruim opgevat. In voorkomende gevallen kan het lijnmanagement ook een afdelingshoofd of een manager van een stafafdeling zijn.

Na het vaststellen wat nodig is – *betrouwbaarheidseisen* –, worden *maatregelen* getroffen, en vervolgens wordt *gecontroleerd* of die maatregelen het gewenste effect sorteren. Deze controle kan aanleiding geven tot bijsturing in de maatregelen. Ook kan uit een *evaluatie* blijken dat het totaal van eisen, maatregelen en controle aan revisie toe is. Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor een adequaat beveiligingsniveau, dat voldoet aan de zes eisen uit het VIR 2007. Wij hebben de invulling van verantwoordelijkheden getoetst aan deze zes punten (zie bijlage 4) en aan een set van gangbare maatregelen van toegangsbeveiliging van informatiesystemen (zie bijlage 2). In bijlage 4 staat ook hoe de verschillende ministeries en baten-lastendiensten scoren.[13]

Enkele ministeries en baten-lastendiensten hebben de gewenste aandacht voor informatiebeveiliging ingebouwd in hun bedrijfsvoering door de kwaliteitscirkel geheel te doorlopen: BuZa, Defensie en IVENT (Defensie). Bij de baten-lastendiensten Logius (Binnenlandse Zaken en Koninkrijksrelaties - BZK) en Centraal Justitieel Incasso Bureau (CJIB) bij het Ministerie van VenJ zien we dat de kwaliteitscirkel bijna geheel wordt doorlopen, met uitzondering van de periodieke evaluatie van het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen (Logius) en de periodieke rapportage aan het lijnmanagement (CJIB). De meeste ministeries en onderzochte baten-lastendiensten echter beschermen hun informatiesystemen nog niet goed of nog niet aantoonbaar tegen risico's van inbraak, misbruik en uitval.
Er wordt vooral slecht gescoord op de volgende twee punten:

- Inzicht in de veiligheidsrisico's van informatiesystemen is onvoldoende;
- Periodieke evaluatie van het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen ontbreekt.

Om inzicht te krijgen in de risico's behoren ministeries en baten-lastendiensten voor hun informatiesystemen risicoafwegingen uit te voeren. Veel ministeries en baten-lastendiensten doen dit niet of doen dit onvoldoende: er is geen inzicht in de uitvoering van risicoafwegingen, risicoafwegingen zijn niet actueel, niet gedocumenteerd of worden alleen voor kritische systemen uitgevoerd. Zonder risicoafwegingen doen ministeries ofwel te veel ofwel te weinig aan beveiliging van informatie. Daardoor verspillen ministeries ofwel tijd en geld, ofwel zij lopen ongewenst risico.

[13] In bijlage 5 staat een grafiek waarin de scores voor zowel beveiligingsbeleid als bescherming van systemen gewogen bij elkaar zijn opgeteld.

De uitvoering van risicoafwegingen is wel op orde bij de Ministeries van AZ, BuZa en Defensie en bij de baten-lastendiensten IVENT (Defensie) – zie kader, Logius (BZK) en CJIB (VenJ).

Goed praktijkvoorbeeld inzicht in veiligheidsrisico's: Dienst Informatievoorziening en -Technologie (IVENT) van het Ministerie van Defensie

Voor alle belangrijke informatiesystemen is een expliciete (navolgbare) risicoafweging uitgevoerd op basis van de binnen Defensie ontwikkelde methode Voorschrift Informatiebeveiliging Rijksdienst Efficiënt en Effectief (VIR E&E analyse). IVENT heeft een speciale afdeling met gecertificeerde medewerkers die de VIR E&E analyse voor alle Defensiesystemen uitvoert.

Doordat een organisatie continu in verandering is (onder meer organisatorisch en technisch) en doordat beveiligingsincidenten altijd kunnen plaatsvinden, is het nodig om periodiek het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen te evalueren. Ook dergelijke periodieke evaluaties zijn nodig om te voorkomen dat ministeries en baten-lastendiensten onbedoeld te veel of te weinig aan de beveiliging van informatie doen.
Bij ons onderzoek zien we dat de meeste ministeries nog niet zover zijn en dat deze laatste stap (het onderdeel '*act*' binnen de PDCA – cyclus) in de kwaliteitscirkel nog niet wordt gezet of niet aantoonbaar wordt gezet.
De periodieke evaluatie is wel op orde bij de Ministeries van Buitenlandse Zaken, Defensie – zie kader – en Financiën (Belastingdienst) en de baten-lastendiensten IVENT (Defensie), Dienst Uitvoering Onderwijs (DUO) van het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en CJIB (VenJ).

Goed praktijkvoorbeeld periodieke evaluatie van betrouwbaarheidseisen en beveiligingsmaatregelen: Ministerie van Defensie

Risicoanalyses volgens de methode VIR Efficiënt en Effectief (VIR E&E analyses) worden eens per drie jaar herzien. Accreditaties en IATO's (*Interim Approval to Operate)* zijn voorzien van een einddatum. Een IATO wordt afgegeven als nog niet alle maatregelen zijn geïmplementeerd en dit niet tot grote risico's leidt. Als de termijn van de accreditatie of IATO verstreken is, dan moet het accreditatieproces – inclusief de VIR E&E analyse – opnieuw worden doorlopen.

4 Vertrouwensfuncties

Mensen die een vertrouwensfunctie bekleden dragen een bijzondere verantwoordelijkheid. Ze hebben toegang tot gevoelige informatie of staatsgeheimen of doen werk dat van vitaal belang is voor de instandhouding van het maatschappelijk leven of werk dat hoge eisen stelt aan hun integriteit. Om er zeker van te zijn dat mensen in vertrouwensfuncties betrouwbaar zijn, moeten ze gescreend worden door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Medewerkers van het Ministerie van Defensie moeten gescreend worden door de MIVD. Ministeries dienen volgens de Wet veiligheidsonderzoeken een actueel overzicht te hebben van de functies die gelden als 'vertrouwensfunctie'. Voordat iemand benoemd wordt op een vertrouwensfunctie moet het ministerie hem/haar aanmelden bij de AIVD voor een veiligheidsonderzoek. De medewerker kan pas aan het werk op deze functie als de AIVD een Verklaring van Geen Bezwaar (VGB) heeft afgegeven. Het is strafbaar iemand zonder VGB in een vertrouwensfunctie aan het werk te laten gaan.
Wij hebben onderzocht of ministeries aan bovenstaande eisen voldoen. Met uitzondering van de Belastingdienst hebben alle ministeries conform de Wet veiligheidsonderzoeken in overeenstemming met de AIVD functies aangewezen als vertrouwensfunctie.
Bij de meeste ministeries wordt een deel van de vertrouwensfuncties uitgeoefend zonder voorafgaande screening door de AIVD. Dit wordt veelal veroorzaakt doordat er geen sluitende administratie wordt bijgehouden (zie tabel op de volgende bladzijde).

Vaststelling van vertrouwensfuncties en screening van medewerkers in vertrouwensfuncties bij onderzochte departementen

Ministeries	Vertrouwens-functies vastgesteld	Aantal vertrouwens-functies	Aantal niet gescreende medewerkers op vertrouwensfunctie*	Sluitende administratie
AZ	Ja	144	5**	Nee
BZK	Ja	635	22**	Nee
BuZa	Ja	448	5	Ja
Defensie	Ja	4877	0	Ja
EL&I	Ja	467	47**	Nee
Financiën (kernministerie)	Ja	115	28**	Nee
Financiën Belastingdienst	Nee	Onbekend		n.v.t.
IenM	Ja	532	130**	Nee
OCW	Ja	78	4	Ja
SZW	Ja	388	3	Ja
VenJ	Ja	210	40**	Nee
VWS	Ja	214	34	Nee

* Berekening percentage 'niet-gescreend' is op basis van deze gegevens niet mogelijk, omdat vaak meer medewerkers op één vertrouwensfunctie werkzaam zijn.

** Schatting op basis van een steekproef.

De Belastingdienst heeft voor het laatst in april 2005 vastgesteld welke functies als een vertrouwensfunctie moeten worden aangemerkt. Er hebben sindsdien enkele organisatorische veranderingen plaatsgevonden waardoor de vertrouwensfuncties opnieuw aangewezen moeten worden. De Belastingdienst heeft vooralsnog verzuimd de lijst met vertrouwensfuncties te actualiseren. Hierdoor ontbreekt het inzicht voor welke functies een screening moet worden uitgevoerd. Dit merken wij aan als een onvolkomenheid in de bedrijfsvoering.
Bij het Ministerie van Defensie blijken grote achterstanden te bestaan in het uitvoeren van veiligheidsonderzoeken door de MIVD. Ook dat hebben wij als een onvolkomenheid aangemerkt. Tegelijkertijd fungeert het Ministerie van Defensie ook als goed voorbeeld. Het heeft een goed systeem om te bewaken dat veiligheidsonderzoeken worden uitgevoerd. In dit systeem signaleert het personeelsinformatiesysteem plaatsingen op vertrouwensfuncties. Wij hebben vastgesteld dat in het personeelsinformatiesysteem (P-Direkt) van de andere departementen ook een dergelijke signalering is ingebouwd, maar dat de standaardrapportages voor managers en controllers desondanks geen inzicht geven in plaatsingen op vertrouwensfuncties. We bevelen de andere ministeries aan om te bewerkstelligen dat de rapportagestructuur van P-Direkt op dit punt wordt aangepast.

5 Reactie ministers en nawoord Algemene Rekenkamer

We hebben deze rapportage op 13 april 2012 voorgelegd aan alle ministers. De ministers van BZK, BuZa, IenM, SZW en VWS hebben geen specifieke reactie gegeven.
De minister van AZ heeft op 16 april 2012 met instemming gereageerd op de positieve vermelding voor zijn departement. Ook de minister van Defensie heeft laten weten verheugd te zijn met de positieve vermelding, in een bijlage bij de reactie op het Rapport bij het Jaarverslag van Defensie, van 23 april jl.
De ministers van EL&I en van OCW hebben laten weten de bevindingen te onderkennen en de aanbevelingen over te nemen, respectievelijk in een brief van 25 april jl. en in een bijlage bij de reactie van op het Rapport bij het jaarverslag van 26 april jl.
De ministers van Financiën en van VenJ hebben gereageerd op het overzicht van onze onderzoeksresultaten betreffende vertrouwensfuncties in hoofdstuk 4. De betreffende teksten nemen we hieronder integraal op, gevolgd door ons nawoord.
Alle genoemde reacties staan integraal op www.rekenkamer.nl.

Reactie minister van Financiën
De minister van Financiën schrijft in zijn reactie op de webpublicatie van 25 april:
'In mijn reactie op het rechtmatigheidsonderzoek ben ik reeds ingegaan op de aandachtspunten en de onvolkomenheid. Kortheidshalve verwijs ik naar deze reactie. Ten aanzien van de vertrouwensfuncties wil ik graag nog het volgende opmerken.
In de tabel wordt geconstateerd dat de administratie van de ingestelde veiligheidsonderzoeken niet sluitend is. Deze constatering is juist. De lacunes worden inmiddels verholpen.
De tabel suggereert ook dat een groot aantal vertrouwensfuncties wordt bezet door medewerkers die niet zijn gescreend. Deze bevinding van de Rekenkamer was aanleiding voor een nader onderzoek. Daarbij bleek dat de lacunes in de administratie en de procedure weliswaar tot dit beeld konden leiden, maar dat in de praktijk alle medewerkers die daadwerkelijk een vertrouwensfunctie vervulden over een Verklaring van geen bezwaar beschikten.

De Belastingdienst is in de zomer van 2011 gestart met een integrale inventarisatie van vertrouwensfuncties; een eerdere inventarisatie was verouderd. Inmiddels is de interne inventarisatie zo goed als afgerond en zal in overleg met de AIVD nog in 2012 tot aanwijzing worden overgegaan.'

Nawoord Algemene Rekenkamer
Wij waarderen de inspanning van de minister om de administratie van de vertrouwensfuncties bij het kernministerie op orde te brengen en een lijst met vertrouwensfuncties vast te stellen bij de Belastingdienst. De minister geeft aan dat in de praktijk alle medewerkers die daadwerkelijk een vertrouwensfunctie vervulden over een Verklaring van Geen Bezwaar beschikten. In ons onderzoek stelden wij vast dat enkele medewerkers op een vertrouwensfunctie werkzaam waren in afwachting van deze verklaring. Wij wijzen erop dat de Wvo daar geen ruimte voor biedt.

Reactie minister van VenJ
In bijlage 4 bij de reactie op het Rapport bij het Jaarverslag 2011 van VenJ gaat de minister van VenJ in op de webpublicatie. Hij schrijft:
'Uw achtergronddocument bevat op pagina's 8 en 9 een tabel met vertrouwensfuncties per departement.
Het valt mij op dat departementen kennelijk verschillend zijn omgegaan met de vraag naar aantallen vertrouwensfuncties. Mijn ministerie heeft het feitelijke aantal aangewezen vertrouwensfunctie opgegeven; enkele andere departementen lijken het aantal vertrouwensfuncties omgerekend in fte's te hebben opgegeven. Dit duidt op een inconsistentie in opzet en met name in de uitvoering van het onderzoek en heeft tot gevolg dat het een vertekend beeld oplevert van de situatie bij de verschillende departementen. Een eenduidige opgave van of feitelijke aangewezen vertrouwensfuncties of van vertrouwensfuncties berekend in fte's voor alle departementen zou zeer wenselijk zijn.'

Nawoord Algemene Rekenkamer
De minister zegt dat ons rapport een vertekend beeld geeft. In ons onderzoek zijn wij aan de hand van de beschikking van de verschillende ministers nagegaan welke functies zij als vertrouwensfuncties hebben aangemerkt. Vervolgens zijn wij nagegaan of voor deze functies een VGB aanwezig is. Wij hebben hiervoor gebruik gemaakt van de administraties van de ministeries en daarnaast bij een aantal ministeries van een steekproef. Of een vertrouwensfunctie betrekking heeft op een hele of een halve fte is niet relevant.

Bijlage 1 Vragenlijst informatiebeveiliging en vertrouwensfuncties

Voor het onderzoek informatiebeveiliging is de onderstaande lijst met vragen gehanteerd. In deel 1 van de lijst (Kwaliteit Informatiebeveiligingsbeleid) wordt ingegaan op de opzet van informatiebeveiliging, maar bij enkele vragen ook op de werking van beveiligingsmaatregelen, zoals bij de vragen 1.5 en 1.8. In deel 2 (Beveiliging van informatiesystemen) staat de goede werking van de informatiebeveiligingsmaatregelen centraal. We wilden nadrukkelijk nagaan of specifieke beveiligingsmaatregelen[14] voor een kritisch informatiesysteem effect sorteren, maar vanwege de vergelijkbaarheid tussen ministeries hebben we uiteindelijk voor een kritisch informatiesysteem een aantal gangbare maatregelen voor toegangsbeveiliging onderzocht. Behalve dat een organisatieonderdeel deze maatregelen genomen moest hebben en eventueel uitgewerkt moest hebben in procedures en werkinstructies, moest ook aantoonbaar zijn dat het organisatieonderdeel volgens die maatregelen werkt (naleving van de maatregelen).

[14] Dit kunnen maatregelen zijn die opgenomen zijn in de technische specificaties van een informatiesysteem, zoals bij integriteitcontroles en maatregelen op het gebied van de beschikbaarheid van hardware, maar ook beveiligingsmaatregelen die deel uitmaken van contracten (bij verwerving). Tevens zijn er maatregelen voor de procedures bij het gebruik van het informatiesysteem.

1. Kwaliteit Informatiebeveiligingsbeleid	
1.1 Is een informatiebeveiligingsbeleid geformuleerd en door de SG vastgesteld?	VIR, art. 3
1.2 Zijn de in wet- en regelgeving verankerde aspecten in dit beleid geïncorporeerd?[15]	BVR; VIR, art. 3 en VIR-BI, art. 13
1.3 Is er een aantoonbare aansluiting tussen het informatiebeveiligingsbeleid en het integrale beveiligingsbeleid?[16]	VIR, art. 3 lid a
1.4 Is de organisatie van de (informatie)beveiligingsfunctie[17] beschreven, waaronder de bijbehorende taken, verantwoordelijkheden en bevoegdheden?	VIR, art. 3, lid b
1.5 Is de procedure met betrekking tot beveiligingsincidenten vastgelegd en uitgedragen?[18]	VIR, art 3, lid b
1.6 Is er een actueel overzicht van alle informatiesystemen en informatieketens en zijn de verantwoordelijkheden hiervoor toegewezen aan lijnmanagers?	VIR, art. 3, lid c
1.7 Wordt binnen het ministerie gewerkt met een gemeenschappelijk stelsel van betrouwbaarheidseisen, lees: baseline informatiebeveiliging	VIR, art. 3, lid d
1.8 Is er een programma voor de bevordering van het beveiligingsbewustzijn? Zijn de maatregelen uit het programma door betrokken organisatieonderdelen uitgevoerd?	VIR, art. 3, lid f
1.9 Is de wijze van toezicht op de uitvoering van het beveiligingsbeleid beschreven?	BVR; VIR, art. 3, lid e en VIR-BI, art. 14, lid 3
1.10 Is er een evaluatie van het informatiebeveiligingsbeleid (inclusief de opvolging van bevindingen ervan) beschreven en wordt deze uitgevoerd?	VIR, art. 3, lid e
2. Beveiliging informatiesystemen	
2.1 Is voor elk informatiesysteem een expliciete (navolgbare) risicoafweging uitgevoerd?	VIR, art. 4, lid a
2.2 Is de totstandkoming van de betrouwbaarheidseisen navolgbaar, gedocumenteerd en zijn deze eisen vastgesteld?	VIR, art. 4, lid a
2.3 Zijn de te treffen beveiligingsmaatregelen aantoonbaar (d.w.z. opzet, bestaan en werking kunnen worden vastgesteld) vastgelegd en uitgevoerd?	VIR, art. 4, lid b
2.4 Zijn er controletaken belegd en wordt toegezien op de uitvoering van de controle om de aanwezigheid en de naleving van de beveiligingsmaatregelen vast te stellen?	VIR, art. 4, lid c
2.5 Vindt er periodieke rapportage aan en door het lijnmanagement plaats over de uitvoering van het beveiligingsbeleid?	VIR, art. 4, lid d VIR, art. 2, lid 3
2.6 Wordt het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen periodiek geëvalueerd en leidt deze evaluatie daar waar nodig tot bijstelling?	VIR, art. 4, lid d
3. Uitvoering Wet veiligheidsonderzoeken	
3.1 Zijn de vertrouwensfuncties vastgesteld?	Wvo, art. 3, eerste lid
3.2 Is voor elke functionaris die werkzaam is in een vertrouwensfunctie een verklaring van geen bezwaar afgegeven?	Wvo, art. 4, derde lid

[15] Zie de afzonderlijke tabel van toepasselijke wet- en regelgeving.

[16] Het ministeriële integrale beveiligingsbeleid zoals bedoeld in het Beveiligingsvoorschrift 2005, omvat naast informatiebeveiliging tevens de beveiliging van materieel en personeel.

[17] De term (informatie)beveiligingsfunctie omvat het geheel aan functies binnen een organisatie en de taken die bij die functies horen.

[18] Het uitdragen van de procedure houdt in dat medewerkers op de hoogte zijn van de procedure en dienovereenkomstig handelen.

Bijlage 2 Maatregelen voor toegangsbeveiliging

Controle van maatregelen ter bescherming van informatiesystemen over 2011		
	Maatregelen	**Toetsing**
1	Via periodieke controles (denk aan interne controle, penetratietesten of specifieke audits, onder meer van de AD) worden de maatregelen van toegangscontrole op hun werking getest.	Documentatie hiervan (laatste 2 of 3 rapporten)
1.1	Toegangscontrole - Kwaadaardige software	
1.1.1	Op elke server en/of werkstation (PC, laptop, etc.) vindt controle plaats op kwaadaardige software en toegang via (bijvoorbeeld) USB-poorten, cd-rom of e-sata van werkstations is geblokkeerd.	Uitdraai van instellingen (filter voor netwerk)
1.1.2	De controlesoftware op kwaadaardige software is zodanig ingesteld dat downloads en email (inclusief attachments) op virussen worden gecontroleerd.	Uitdraai van instellingen antivirussoftware en/of firewall (filter voor toegang)
1.2	Toegangscontrole - Gebruikerswachtwoorden	
1.2.1	Bij afgifte van tijdelijke wachtwoorden wordt direct wijziging afgedwongen.	Uitdraai instellingen besturingssysteem of betreffende applicatie
1.2.2	Het wachtwoordsysteem voldoet minimaal aan de volgende eisen: - minimumlengte (8 à 10 karakters voor gebruikers en langer voor beheerders) - regulier wijzigen van wachtwoorden (voor gebruikers minstens eenmaal per 3 maanden, voor beheerders minstens eenmaal per maand) - hergebruik van wachtwoorden voorkomen (d.m.v. een historie van minimaal 10 wachtwoorden) - voldoende kwaliteit van wachtwoorden: niet gebaseerd op data (jaren, maanden, dagen), niet gebaseerd op namen van dienstonderdelen, niet uitsluitend numerieke of alfabetische tekens, e.d.	Uitdraai instellingen besturingssysteem of betreffende applicatie
1.3	Toegangscontrole - besturingssysteem / netwerk	
1.3.1	Mogelijkheden voor gebruikers om verbinding te maken met netwerken worden beperkt en zijn in lijn met het toegangscontrolebeleid.	Uitdraai instellingen besturingssysteem of betreffende applicatie
1.3.2	Gebruikers hebben alleen toegang tot die diensten waar zij specifiek voor zijn geautoriseerd.	Uitdraai autorisatietabel + steekproef autorisatietoekenningen

1.3.3	Gebruikers krijgen uitsluitend toegang tot het netwerk en hun computer door middel van een standaard aanlogprocedure	Toon aan
1.3.4	Bij het inloggen worden alleen de noodzakelijke data-input velden weergegeven (en dus geen hulpboodschappen die kunnen worden benut door onbevoegden).	Toon aan
1.3.5	Alle gebruikers (inclusief technisch IT-personeel) hebben een uniek user-id, zodat alle activiteiten naar de persoon kunnen worden herleid. (óf: het gebruik van een algemeen beheerders-id wordt procedureel beperkt.)	Log gebruik beheerders-id en log gebruik persoonlijke id's beheerders + procedure voor gebruik beheerders-id
1.3.6	Er is een schermbeveiligingsprogramma ingesteld met een maximumtijd van 15 minuten.	Uitdraai instellingen besturingssysteem of betreffende applicatie en test ter plaatse
1.3.7	Het geïnstalleerde schermbeveiligingsprogramma kan alleen door de gebruiker met zijn eigen wachtwoord worden ontgrendeld.	Uitdraai instellingen besturingssysteem of betreffende applicatie
1.4	**Toegangscontrole - Thuiswerkfaciliteit**	
1.4.1	Voor de thuiswerkfaciliteit krijgen gebruikers uitsluitend toegang tot het netwerk door middel van two or three factor authentication.	Toon aan
1.4.2	Bestaan er uitzonderingen op het bovengenoemde authenticatiebeleid voor thuiswerkfaciliteiten? (bijvoorbeeld voor beheerders)	Toon aan
2	Er worden loggings bijgehouden van verkeerde inlogpogingen en de handelingen in het kritische systeem, die gebruikt kunnen worden voor preventief en repressief integriteitsbeleid (netwerk, kritisch systeem).	Toon aan (zie onder)

2.1	Loggings bevatten de volgende relevante gegevens
	• Gebruikersidentificatie;
	• Identificatie server/werkstation;
	• Datum, tijd en details van gebeurtenissen, namelijk
	  ○ Geslaagde en mislukte pogingen voor toegang;
	  ○ Toekennen rechten/autorisaties
	  ○ Veranderingen aan de configuratie en
	• Gebruik van de volgende privileges: a, b, c
		Toon instellingen logging + voorbeeld logging van een dag/week

2.2	De loggings worden gebruikt ten behoeve van preventief en repressief integriteitsbeleid.	Toon procedure en laatste (2) check(s)

Bijlage 3 Normen en scores kwaliteit informatiebeveiligingsbeleid

Op grond van VIR 2007 en VIR-BI moet het informatiebeveiligingsbeleid voldoen aan de volgende eisen:

1. Het beleid is op het hoogste managementniveau vastgesteld, waardoor het hoogste management zich betrokken toont bij het beleid en verantwoordelijkheid draagt voor het beleid;
2. Het beleid is aangepast aan de meest recente inzichten in wet- en regelgeving;
3. Het beleid voor informatiebeveiliging is geïntegreerd in het algemene beveiligingsbeleid;
4. Het is duidelijk wie voor welk deel van de informatiebeveiliging verantwoordelijk is en wat de bevoegdheden zijn vanuit deze verantwoordelijkheden;
5. Het ministerie beschikt over een standaardprocedure om te reageren op beveiligingsincidenten zoals inbraakpogingen;
6. Het is voor alle informatiesystemen en informatieketens duidelijk welk organisatieonderdeel verantwoordelijk is voor de informatiebeveiliging;
7. Het ministerie werkt met minimum betrouwbaarheidseisen en betrouwbaarheidsmaatregelen die voor alle systemen gelden;
8. Medewerkers leren hoe ze veilig kunnen omgaan met informatie;
9. Het ministerie controleert dat het informatiebeveiligingsbeleid wordt uitgevoerd en dat dat medewerkers veilig omgaan met informatie;
10. Het informatiebeveiligingsbeleid wordt periodiek geëvalueerd.

Uit de tabel blijkt dat de ministeries en baten-lastendiensten relatief slecht scoren op onderdeel 6 (de toewijzing van de verantwoordelijkheid voor informatiesystemen en informatieketens aan organisatieonderdelen) en op onderdeel 10 (periodieke evaluatie van het informatiebeveiligingsbeleid).

Scores ministeries en baten-lastendiensten op bovenstaande eisen voor informatiebeveiligingsbeleid

	1	2	3	4	5	6	7	8	9	10
AZ	☺	😐	😐	😐	☺	☹	☺	☺	☺	☺
BZK (kernministerie)	☺	☹	☺	😐	☺	😐	☹	☺	☹	☹
BZK (Logius)	☺	😐	☺	😐	☺	😐	☹	☺	☺	☹
BuZa	☺	😐	☺	☺	☺	☺	☺	😐	☺	☺
Defensie (kernministerie)	☺	☺	☺	☺	☺	☺	☺	☺	☺	☺
Defensie (IVENT)	☺	☺	☺	☺	☺	☺	☺	☺	☺	☺
EL&I (kernministerie)	😐	😐	☺	😐	☺	😐	☺	😐	😐	☹
EL&I (DICTU)	☺	☺	☺	☺	☺	☺	☺	☺	☺	☺
Financiën (kernministerie)	☺	☺	☺	☺	😐	😐	☺	☺	☺	☺
Belastingdienst	☺	☺	☺	☺	☺	☺	☺	☺	☺	☺
I&M (kernministerie)	☺	😐	☺	😐	😐	😐	☺	☺	😐	☹
I&M (RWS)	☺	😐	☺	😐	☺	☺	☺	☺	☺	☹
OCW (kernministerie)	☺	☺	☺	☺	☺	☹	☺	☺	☺	😐
OCW (DUO)	☺	☺	☺	☺	😐	😐	☺	☺	☺	☹
SZW (kernministerie)	☺	☺	☺	☺	☺	☺	☺	☺	☺	😐
Agentschap SZW	☺	☺	☺	😐	☺	☺	☺	☺	☺	☹
V&J (kernministerie)	☺	😐	☺	☺	😐	☺	☺	☺	😐	☹
V&J (CJIB)	☺	😐	😐	😐	☺	☺	☺	😐	☺	☹
VWS (kernministerie)	☺	😐	☺	☺	☺	😐	☺	😐	☺	☹
VWS (RIVM)	☺	☺	☺	☺	☺	😐	☺	😐	☺	😐
VWS (CBG)	☺	☺	☺	☺	☺	☹	☺	☺	☺	😐

Legenda

☺ voldoende 😐 voor verbetering vatbaar ☹ sterk voor verbetering vatbaar

De nummering boven de kolommen correspondeert met de nummering van de door ons onderzochte onderdelen van het informatiebeveiligingsbeleid.

Bijlage 4 Normen en scores bescherming van informatiesystemen

Op grond van het VIR 2007 vindt informatiebeveiliging plaats via de kwaliteitscirkel van Deming (Plan Do Check Act – cyclus). Bij het goed doorlopen van deze cirkel is altijd sprake van een goede beveiliging en voldoet de beveiliging aan de volgende eisen:

1. De verantwoordelijke organisatieonderdelen hebben de veiligheidsrisico's van de informatiesystemen in beeld (onderdeel 'plan' binnen de PDCA – cyclus);
2. Ze weten (daardoor) wat de kwetsbaarheden van deze systemen zijn en welke betrouwbaarheid van het systeem daarvoor nodig is (onderdeel 'plan' binnen de PDCA – cyclus);
3. Ze weten dat noodzakelijke gangbare maatregelen van logische toegangsbeveiliging worden uitgevoerd en goed werken (onderdeel 'do' binnen de PDCA – cyclus);
4. Ze weten dat noodzakelijke specifieke beveiligingsmaatregelen worden uitgevoerd en goed werken (onderdeel 'do' binnen de PDCA – cyclus);
5. Er zijn periodieke rapportages over informatiebeveiliging (onderdeel 'check' binnen de PDCA – cyclus);
6. Er worden evaluaties uitgevoerd om te zien of de beveiliging goed werkt en eventueel bijgesteld moet worden (onderdeel 'act' binnen de PDCA – cyclus).

Uit de tabel blijkt dat de ministeries en baten-lastendiensten relatief slecht scoren op onderdeel 1 (inzicht van organisatieonderdelen in veiligheidsrisico's van systemen) en op onderdeel 6 (het uitvoeren van evaluaties van de betrouwbaarheidseisen en beveiligingsmaatregelen voor informatiesystemen).

Scores ministeries en baten-lastendiensten op bovenstaande eisen voor de bescherming van informatiesystemen

	1	2	3	4	5	6
AZ						
BZK (kernministerie)						
BZK (Logius)						
BuZa						
Defensie (kernministerie)						
Defensie (IVENT)						
EL&I (kernministerie)						
EL&I (DICTU)						
Financiën (kernministerie)						
Belastingdienst						
I&M (kernministerie)						
I&M (RWS)						
OCW (kernministerie)						
OCW (DUO)						
SZW (kernministerie)						
Agentschap SZW						
V&J (kernministerie)						
V&J (CJIB)						
VWS (kernministerie)						
VWS (RIVM)						
VWS (CBG)						

Legenda

 voldoende voor verbetering vatbaar sterk voor verbetering vatbaar

De nummering boven de kolommen correspondeert met de nummering van de door ons onderzochte onderdelen van het informatiebeveiligingsbeleid.

Bijlage 5 Scores informatiebeveiliging (beveiligingsbeleid *en* bescherming informatiesystemen)