Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

14

Vragen van het lid **Rog** (CDA) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het bericht «Duo niet goed beveiligd»* (ingezonden 12 augustus 2013).

Antwoord van Minister **Bussemaker** (Onderwijs, Cultuur en Wetenschap) (ontvangen 17 september 2013).

Vraag 1
Heeft u kennis genomen van het artikel «DUO niet goed beveiligd» op de website van ScienceGuide?[1]

Antwoord 1
Ja

Vraag 2
Klopt het dat de Auditdienst Rijk (ADR) in 2011 al heeft vastgesteld dat het informatiebeveiligingsplan niet volledig was afgerond? Klopt het dat eind 2012 er nog steeds sprake is van dat DUO «voortdurend risico's op het gebied van informatiebeveiliging loopt»? Welke concrete acties heeft u ondernomen of gaat u ondernemen om het tactische security-management te verbeteren?

Antwoord 2
Informatiebeveiliging vraagt continu om de volle aandacht. De bevindingen van de Auditdienst Rijk (ADR) zijn daarbij van belang en de adviezen worden opgevolgd. De ADR heeft in zijn rapport over 2011 inderdaad vastgesteld dat het informatiebeveiligingsplan niet volledig was afgerond en dat er nog enkele onderdelen ontbraken, namelijk koppeling met het OCW-informatiebeveiligingsbeleid, een controlcyclus rond de informatiebeveiliging en een «beveiligingsbewustzijnsprogramma».
In het rapport over 2012 heeft de ADR gesteld dat DUO Groningen risico's op het gebied van informatiebeveiliging loopt. Daarbij is de situatie door de ADR ingeschaald als «gemiddeld».[2] Van voortdurende risico's op het gebied van informatiebeveiliging is naar mijn mening geen sprake, het securitymanagement is operationeel op orde.

[1] ScienceGuide.nl, 8 augustus 2013
[2] Samenvattend auditrapport 2012 OCW, blz. 13.

ah-tk-20132014-14
ISSN 0921 - 7398
's-Gravenhage 2013

Het ADR-advies betreft de verbetering van het tactisch securitymanagement en het opstellen van een bedrijfscontinuïteitsplan (BCP).
Overeenkomstig het advies werkt DUO aan het inrichten van het tactisch securitymanagement, waarbij de Baseline Informatiebeveiliging Rijksoverheid als uitgangspunt wordt genomen. In opvolging van het advies is het management met de Taskforce Informatiebeveiliging op voldoende niveau betrokken bij het bewaken van de voortgang en het uitvoeren van de controlcyclus.
Dit is gerealiseerd door het voorzitterschap van de Hoofddirecteur Bedrijfsvoering en de deelname van de Chief Information Officer, de Centrale Security Officer en de manager van afdeling Informatie- en Communicatietechnologie. De ADR zal voor zijn rapportage over 2013 bezien of er voldoende voortgang is geboekt bij het inrichten van het tactisch securitymanagement.
Overeenkomstig het tweede advies wordt gewerkt aan verbetering van het bedrijfscontinuïteitsplan. Een volledig bedrijfscontinuïteitsplan vergroot immers de kans dat in het geval van een calamiteit de juiste procedures worden gevolgd. Om te borgen dat er in geval van incidenten juist wordt gehandeld, heeft DUO ervoor gekozen om bedrijfscontinuïteitsmanagement (BCM) in te richten. Eind 2013 worden bedrijfscontinuïteitsplannen opgeleverd voor de meest kritische bedrijfsprocessen. De ADR zal ook op dit punt bezien of er voldoende voortgang is geboekt.

Vraag 3
Klopt het dat voor het bewaken van de voortgang en het uitvoeren een controlcyclus het auditrapport stelt dat het essentieel is dat het management van DUO «zichtbaar betrokken is»? Deelt u de stelling dat het management meer «zichtbaar betrokken» moet zijn? Zo ja, hoe wendt u uw invloed aan om dit te realiseren?

Antwoord 3
Zie het antwoord op vraag 2.

Vraag 4
Klopt het dat in het aangehaalde auditrapport staat dat het ontbreken van een bedrijfscontinuïteitsplan (BCP) de kans vergroot dat bij een calamiteit niet de meest doelmatige procedures worden gevolgd? Klopt het dat dit kan leiden tot een groot politiek afbreukrisico? Bent u voornemens om nog dit jaar capaciteit vrij te maken voor het opstellen van een overkoepelend BCP, zoals in het auditrapport wordt aanbevolen?

Antwoord 4
Zie het antwoord op vraag 2.

Vraag 5
Klopt het dat in het auditrapport expliciet gewaarschuwd wordt voor de risico's op het gebied van informatiebeveiliging, mede door de vele klantrelaties en de sterke afhankelijkheid van ICT? Deelt u de mening dat invoering van het leenstelsel deze kwetsbaarheid verder zou kunnen vergroten en studenten daardoor nog meer risico lopen dat hun vertrouwelijke gegevens in handen komen van onbevoegden?

Antwoord 5
Zie het antwoord op vraag 2.
Nee, ik deel die mening niet. Er is geen directe relatie tussen de genoemde risico's en het sociaal leenstelsel. Met het sociaal leenstelsel verandert de aard en omvang van de gegevens niet significant.