Ministerie van Onderwijs, Cultuur en Wetenschap

> Retouradres Postbus 16375 2500 BJ Den Haag

De voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
312661

Uw referentie
2011Z12556

Datum 1 juli 2011
Betreft Vragen van de leden Van der Ham en Hachchi (beiden D66)

Hierbij zend ik u het antwoord op de vragen van de Kamerleden Van der Ham en Hachchi (D66) aan de ministers van Onderwijs, Cultuur en Wetenschap en van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat de website van DUO onveilig is (ingezonden 14 juni 2011).

De vragen werden mij toegezonden bij uw bovenaangehaalde brief met kenmerk 2011Z12556.

De minister van Onderwijs, Cultuur en Wetenschap,
mede namens de minster van Binnenlandse Zaken en Koninkrijksrelaties,

Marja van Bijsterveldt-Vliegenthart

Antwoorden op de schriftelijke vragen van de Kamerleden Van der Ham en Hachchi (D66) aan de ministers van Onderwijs, Cultuur en Wetenschap en van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat de website van DUO onveilig is (ingezonden 14 juni 2011 kenmerk 2011Z12556)

Vraag 1
Wat is uw reactie op het bericht dat er voor de tweede keer in een half jaar een lek zit in de website van de Dienst Uitvoering Onderwijs (DUO)?

Ik betreur dat er voor de tweede keer een incident op de website van DUO heeft plaatsgevonden. Gebruikers van deze site moeten kunnen rekenen op betrouwbare en beveiligde informatie.

Vraag 2
Hoe kan het dat de website van DUO niet bestand blijkt tegen hackers, ondanks dat u eerder aangaf opdracht te hebben gegeven "een externe audit uit te voeren" die tot aanbevelingen kon leiden "om dit soort problemen te voorkomen"?

Deze website van DUO wordt diverse malen per maand aangevallen door hackers. De site is beveiligd met een systeem dat hack-pogingen registreert en signaleert en (wijzigingen van) systemen worden getest op veiligheid. Het incident van 7 juni jl. betreft een actie van een hacker die de veiligheid van de DUO-site heeft getest door een eigen pagina op de site te plaatsen. Dit had niet mogen gebeuren. Het bewuste lek is per omgaande gerepareerd. DUO heeft vervolgens al haar websites gecontroleerd op mogelijke beveiligingslekken en waar nodig maatregelen getroffen.
De huidige hack-aanval op de site van DUO verschilt van het incident van 5 november vorig jaar. Toen was er sprake van een interne fout in de webapplicatie "Mijn DUO", waardoor vijf studenten per ongeluk de gegevens van een ander hebben kunnen inzien. De externe audit op dit eerdere incident is in de eerste maanden van 2011 uitgevoerd door PWC. De aanbevelingen uit deze audit zijn door DUO overgenomen.

Vraag 3
Hoe verhoudt dit voorval zich tot uw toezegging om studenten "een betrouwbaar systeem te kunnen bieden"?

Het systeem waarmee studenten transacties doen met DUO is betrouwbaar. DUO doet er alles aan om te zorgen dat de informatiebeveiliging zodanig is ingericht dat er geen derden via de site bij de gegevens kunnen komen.

Vraag 4
Wat gaat u doen om te zorgen dat deze problemen zich in de toekomst niet nogmaals voordoen?

De aanbevelingen uit de audit, zoals genoemd in het antwoord op vraag 2, hebben DUO hierbij geholpen. Dit betekent dat DUO investeert in preventie om de kans op incidenten te minimaliseren en op het versterken van het vermogen tot incidenten snel en gestructureerd af te handelen en de gevolgschade te beheersen.

Hierbij zal altijd sprake zijn van een afweging van kosten en capaciteit tegen risico's. Het ontstaan van incidenten kan niet voor 100 procent worden voorkomen, zoals ook recente voorbeelden in andere sectoren illustreren (Nintendo, Sony, de RABO-bank en de CIA).
Ten slotte heeft DUO aangifte gedaan omdat het hacken van een site strafbaar is.

Vraag 5
Zijn er andere overheidswebsites die evenzeer kwetsbaar zijn? Waar blijkt dit uit?

Mij is niet bekend of ook andere overheidsorganisaties last hebben gehad van dergelijke hack incidenten. De medeoverheden hebben ten aanzien van informatiebeveiliging hun eigen verantwoordelijkheid voor wat betreft de interne, ketenonafhankelijke, bedrijfsvoering.

Vraag 6
Op welke wijze wordt het toegezegde onderzoek naar dit lek vormgegeven? Worden daarbij externe experts ingeschakeld?

Zie het antwoord op vraag 2. Bij het onderzoek naar de hack-aanval van 7 juni jl. en bij het treffen van herstelmaatregelen zijn interne en externe experts ingeschakeld.