Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

356

Vragen van de leden **Jan Jacob van Dijk** en **Biskop** (beiden CDA) aan de minister van Onderwijs, Cultuur en Wetenschap over *het artikel «Gevoelige informatie studenten Utrecht jaren openbaar».* (Ingezonden 7 september 2009)

1
Bent u bekend met het artikel «Gevoelige informatie studenten Utrecht jaren openbaar»?[1]

2
Zijn er naast dit geval van lekken van gevoelige informatie van studenten op het internet/intranet nog meer gevallen bekend van onbeveiligde gegevens op het internet/intranet van studenten? Is er een inventarisatie van deze gevallen? Zo ja, is deze inventarisatie ter inzage beschikbaar? Zo nee, is het dan mogelijk dat het ministerie een inventarisatie maakt?

3
Kunt u bevestigen dat de websites doorgaans goed zijn beveiligd, maar dat het vaak ontbreekt aan tijdige updates en zorgvuldig gebruik van de websites door studenten, docenten en andere medewerkers, waardoor de websites onvoldoende beveiligd/veilig blijken te zijn? Welke vormen van voorlichting vanuit het ministerie en/of de instellingen zijn er? Is dit volgens het ministerie voldoende? Zo niet, wat gaat u daar aan doen?

4
Deelt u de mening dat de beveiliging van informatie over studenten, oftewel de privacy van deelnemers aan het onderwijs, een belangrijk aandachtspunt voor instellingen zou moeten zijn? Zo ja, wat gaat u doen om dit onder de aandacht van de instellingen te brengen?

[1] www.elsevier.nl, 2 september 2009: «Gevoelige informatie studenten Utrecht jaren openbaar».

Antwoord

Antwoord van minister **Plasterk** (Onderwijs, Cultuur en Wetenschap) (ontvangen 15 oktober 2009)

1
Ja.

2
Zeer recent is in het Onderwijsblad, een uitgave van de AOb, een onderzoek gepubliceerd naar het lekken van studentgegevens. Uit deze inventarisatie komt naar voren dat van verschillende onderwijsinstellingen studentgegevens op het internet zijn te traceren.[1] In enkele gevallen ging het om informatie die door de student – al dan niet bewust – op het internet was geplaatst. Maar in enkele gevallen ging het om informatie die onbedoeld door de instellingen openbaar was gemaakt. Nadat instellingen door de onderzoekers daarop waren geattendeerd hebben deze instellingen hun werkwijze c.q. hun site aangepast. In het geval zoals beschreven in het bovengenoemd artikel in Elsevier heeft de instelling, zodra het lek was ontdekt, ingegrepen en het lek «gedicht» en de informatie offline gehaald.

3
Ik kan geen oordeel geven over de wijze waarop de websites van de instellingen zijn beveiligd noch over de oorzaken van een eventueel tekortschieten daarvan. Ik acht een goede naleving van de Wet bescherming persoonsgegevens de verantwoordelijkheid van de instellingen voor hoger onderwijs. Ik heb daarin geen bijzondere rol of bevoegdheid. Bij een goede naleving door de instelling past ook de verantwoordelijkheid van de instelling voor het treffen van passende, technische en andersoortige, voorzieningen om de privacy van de betrokkenen te beschermen.
De beveiliging van de informatiesystemen is de verantwoordelijkheid van de instellingen voor hoger onderwijs. De reguliere voorschriften omtrent (de borging van) privacy-gegevens gelden onverkort voor deze instellingen. In die zin zijn de instellingen voor hoger onderwijs

KVR38015
2009Z15886
0910tkkvr356
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2009

niet anders dan andere organisaties die werken met privacy-gevoelige informatie. Uiteraard is de beveiliging van informatie van groot belang, waar serieus aandacht voor moet zijn binnen de instellingen. Binnen de universiteiten en hogescholen worden hiertoe ook initiatieven en werkzaamheden ontplooid. Zo zijn medewerkers actief in het beveiligen van informatie die vanuit de instelling wordt verspreid; gegevens die door de studenten zelf openbaar worden gemaakt vallen daar uiteraard niet onder. Verder komen (medewerkers van) de instellingen sinds een aantal jaren bijeen om kennis en ervaringen uit te wisselen over informatiebeveiliging in het kader van Stichting Surf. Er wordt informatie uitgewisseld over beveiligingsinbreuken, er wordt voorlichting gegeven aan de aangesloten instellingen op het gebied van beveiliging, zowel incidenteel (bij calamiteiten) als structureel (bijvoorbeeld in het geval van verspreiding van kennis over beveiligingslekken in software).

4
Zie mijn antwoord op de vorige vragen.

[1] Uitgave nr. 15, 3 oktober 2009.