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

2454

Vragen van de leden **Biskop** en **Jan de Vries** (beiden CDA) aan de minister van Onderwijs, Cultuur en Wetenschap over *de beveiliging van computernetwerken op middelbare scholen* (ingezonden 1 april 2010).

Antwoord van staatssecretaris **Van Bijsterveldt-Vliegenthart** (Onderwijs, Cultuur en Wetenschap) (ontvangen 18 mei 2010).

Vraag 1
Bent u bekend met het artikel «De script kiddies zien speeltuin in intranet»?[1]

Antwoord 1
Ja.

Vraag 2
Wat is uw mening over het feit dat leerlingen dermate gemakkelijk op computernetwerken van scholen kunnen inbreken dat ze van tevoren proefwerken kunnen inzien, cijfers veranderen, absentiemeldingen verwijderen en roosters wijzigen?

Antwoord 2
Vanzelfsprekend vind ik dat dit niet mag voorkomen. In de recente brief aan uw kamer van 16 april 2010 ben ik uitvoerig ingegaan op de beveiliging van leerlinggegevens naar aanleiding van de vragen van heer Biskop terzake bij de begrotingsbehandeling van 2010, gebaseerd op een onderzoek bij 36 scholen naar de vrije beschikbaarheid van leerlinggegevens via internet. Uit dat onderzoek bleek overigens dat deze gegevens niet vrij beschikbaar zijn via internet, wel bleek dat er beveiligingsfouten in de systemen zitten. In de antwoordbrief is aangegeven dat de onderwijsinstellingen primair verantwoordelijk zijn voor de beveiliging van leerlinggegevens, maar is wel de toezegging gedaan om via DUO in de reguliere communicatie richting administrateurs van de onderwijsinstellingen nog eens te wijzen op het belang van gegevensbeveiliging.

Vraag 3
Wat zegt dit over de borging van de onderwijskwaliteit, zoals die onder andere wordt beoordeeld aan de hand van de gegeven onderwijstijd en de behaalde leerresultaten?

[1] Het Parool, 27 maart 2010.

ah-tk-20092010-2454
ISSN 0921 - 7398
's-Gravenhage 2010

Antwoord 3
Mijn beeld is dat het hier om incidentele gevallen gaat. De borging van de onderwijskwaliteit is daarom mijns inziens niet in het geding.

Vraag 4
Verheugt het u dat een goede moraal sommige leerlingen ervan weerhoudt misbruik te maken van de hun bekende inloggegevens?

Antwoord 4
Ja, dat verheugt mij. Naast een adequate beveiliging van de computernetwerken is het van belang dat er binnen de school goede afspraken worden gemaakt tussen docenten en leerlingen en dat op voorhand helder is wat de consequenties zijn van misbruik/wangedrag. Zie ook mijn antwoord op vraag 7.

Vraag 5
Hoe staat het gegeven dat niet één van de in 2004 en 2007 door Kennisnet onderzochte scholen zijn beveiliging op orde had? Wat is de voortgang op het onderzoeksrapport over internetbeveiliging dat het lid Biskop tijdens de begrotingsbehandeling 2010 aan uw voorganger heeft aangeboden?

Antwoord 5
Voorop staat dat de onderwijsinstellingen hun beveiliging op orde dienen te hebben. Dat vereist voortdurende aandacht. Anderzijds worden in elke organisatie tijdens een audit verbeterpunten gevonden. Geen systeem is waterdicht, en zeker een systeem zoals het onderwijs, dat in principe gekenmerkt wordt door openheid, kan nooit volledig beveiligd worden zonder onbruikbaar te worden. Zolang apple's iPhone of iPad gekraakt wordt op de dag van introductie, beveiliging van paspoorten wordt gebroken en OV chipkaarten binnen weken worden gehackt is duidelijk dat juist ook in onderwijs geen 100% veiligheid realiseerbaar is.

De school moet een afweging maken tussen beveiliging via technologie en via afspraken met docenten en leerlingen.
Een voorbeeld: In de onderwijsomgeving wordt steeds meer gebruik gemaakt van digitaal leermateriaal en applicaties op internet, docenten werken hierin samen met leerlingen en stellen hun eigen faciliteiten hiervoor beschikbaar (laptop met wachtwoord). Dit is het gewenste open karakter van onderwijs. Echter de administratieve omgeving met cijfers, absentie administratie, proefwerken, etc. heeft een heel ander karakter en is strikt bedoeld voor docenten en ondersteunend personeel.
Indien deze omgevingen niet gescheiden worden kan een docent eigenlijk al niet goed meer functioneren. Het dilemma voor de school is dus of ze een open leeromgeving biedt of dat ze alles afschermt om de administratie veilig te houden?
In de brief van 16 april 2010 is antwoord gegeven op de door lid Biskop gestelde vragen tijdens de begrotingsbehandeling van 2010. Zie verder ook mijn antwoord op vraag 7.

Vraag 6
Deelt u de in het artikel geventileerde mening dat tegen hackers met een puzzelmentaliteit geen kruid gewassen is?

Antwoord 6
De beschreven methoden van inbraak illustreren dat we niet met whizzkids te maken hebben. Deze methoden: key-loggers en «meeluisteren» op het draadloze netwerk, staan beschreven op Internet en kunnen door een ieder gebruikt worden. Ook hier manifesteert zich het conflict tussen een open onderwijsomgeving en een veilige administratie. Toegang tot apparatuur biedt de mogelijkheid software te installeren die helpt inbreken (bijv. key-loggers), een vrij toegankelijk draadloos netwerk biedt toegang tot leermateriaal, maar ook de mogelijkheid mee te luisteren naar «vertrouwelijk» verkeer.
In het onderwijs is een open leeromgeving en veel contact met de buitenwereld een uitgangspunt. Systemen kunnen daarom niet simpelweg op slot zoals bij banken, verzekeraars of private ondernemingen. Daarnaast zijn

leerlingen in het middelbaar onderwijs onderdeel van de organisatie. Het betreft een groep slimme, jonge mensen met veel tijd, veelal behoorlijke ICT kennis, de drang zich te bewijzen en een zich nog ontwikkelend normbesef. Misbruik van openheid kan altijd plaatsvinden, dit is niet uniek voor de digitale wereld, getuige sleutelplannen op onderwijsinstellingen en problemen met diefstal van persoonlijke eigendommen van docenten en leerlingen als die niet goed achter slot en grendel worden gehouden.

Vraag 7
Wat kunnen scholen volgens u doen om hun computernetwerken, in het artikel ook wel omschreven als «nog nét geen gatenkaas», beter te beveiligen en daarmee de onderwijskwaliteit beter te waarborgen? Welke rol ziet u hierin voor uzelf en/of voor de Onderwijsinspectie?

Antwoord 7
Betere beveiliging zit zowel in de technologie, als in goede afspraken met docenten en leerlingen, duidelijke verantwoordelijkheden en op voorhand heldere consequenties van misbruik/wangedrag, bijv. toegang ontzeggen tot ICT faciliteiten bij misbruik.
Daarnaast is het scheiden van leeromgeving en administratie van belang, zodat een docent zich veilig kan openstellen tijdens de les en veilig de administratie kan raadplegen/bijwerken. Natuurlijk moeten gegevens vanuit de onderwijssituatie op efficiënte wijze geadministreerd kunnen worden, maar tegelijk moet niet iedereen bij alles kunnen. Dit vergt heldere afspraken over en uitvoering van wie toegang krijgt tot welke gegevens: authenticatie en autorisatie.
Het antwoord ligt niet in 100% beveiliging, maar eerder in goede afspraken met mensen, ondersteund door adequate maatregelen en veiligheidsnetten om incidenten te kunnen signaleren en corrigeren. Denk hierbij aan het terugmelden van wijzigingen in cijfer- en absentieadministratie aan de docent van de betreffende klas/leerling, zodat verificatie van een wijzing mogelijk is.

In de brief van 16 april heb ik u al geïnformeerd over de te nemen maatregelen. Via DUO zullen de onderwijsinstellingen worden gewezen op het belang van gegevensbeveiliging.
Daarnaast wijs ik u op de brief van 14 april 2010 van de Minister van Justitie aan uw Kamer, die mede namens OCW is uitgegaan, over High Tech Crime en Voorlichting. Daarin wordt in de actielijnen weergegeven hoe synergie en effectiviteit van voorlichtingsactiviteiten op het gebied van internetveiligheid versterkt zullen worden.