Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

1572

Vragen van de leden **Westerveld** en **Bouchallikh** (beiden GroenLinks) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het bericht «Omstreden software studenten blijkt onveilig: hackers konden meegluren»* (ingezonden 15 december 2021).

Antwoord van Minister **Dijkgraaf** (Onderwijs, Cultuur en Wetenschap) (ontvangen 4 februari 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1309.

Vraag 1
Bent u bekend met het bericht «Omstreden software studenten blijkt onveilig: hackers konden meegluren»?[1]

Antwoord 1
Ja

Vraag 2
Deelt u de mening dat het zeer onwenselijk is dat vele tienduizenden Nederlandse studenten maandenlang gemakkelijk te hacken zijn geweest, omdat hun opleiding hen verplichtte onveilige antispieksoftware te installeren?

Antwoord 2
Sinds de coronacrisis is het voor onderwijsinstellingen lastiger om tentamens op locatie te organiseren. In sommige gevallen is voor onderwijsinstellingen het gebruik van proctoring software noodzakelijk om de studievoortgang van studenten te garanderen. Indien de gebruikte software achteraf gezien onveilig bleek, dan beschouw ik dat als onwenselijk. De onderwijsinstellingen dienen hierom het gesprek aan te gaan met de softwareleverancier, zodat de software beter beveiligd wordt.

[1] Website RTL Nieuws, 14 december 2021, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5273869/studenten-nederland-proctorio-hacken-plugin-uva

ah-tk-20212022-1572
ISSN 0921 - 7398
's-Gravenhage 2022

Vraag 3
Bent u voornemens om instellingen erop te wijzen dat software zoals Proctorio alleen in uitzonderlijke gevallen moet worden gebruikt, bijvoorbeeld als een student niet fysiek naar een tentamen kan komen vanwege een functiebeperking?

Antwoord 3
Mede op aandringen van uw Kamer heeft mijn ambtsvoorganger in samenspraak met de hoger onderwijsinstellingen in het servicedocument[2] afspraken gemaakt over de inzet van proctoring software. In het servicedocument is onder andere afgesproken dat de inzet van proctoring alleen een geschikte optie kan zijn om een tentamen af te leggen als er geen goed alternatief is. Daarnaast: «voor het juiste gebruik van online surveillance en proctoring dienen instellingen gebruik te maken van de handreikingen van de AP[3] en SURF[4]».
Het inzetten van proctoring kan een oplossing bieden aan studenten die niet naar een instelling kunnen komen. Voorbeelden hiervan zijn studenten met een functiebeperking, maar ook studenten met een kwetsbare gezondheid, mantelzorgers, topsporters en studenten die in quarantaine zitten.

Vraag 4
Is bekend op welke onderwijsinstellingen de software Proctorio op dit moment wordt gebruikt en welke instellingen sinds het begin van de coronapandemie Proctorio hebben ingezet?

Antwoord 4
Bij navraag door de Universiteiten van Nederland (UNL) is gebleken dat negen universiteiten op enig moment de software Proctorio hebben gebruikt. Bij een eerdere rondvraag van de Vereniging Hogescholen (VH) onder 25 hogescholen gaf ongeveer de helft aan gebruik te maken van online proctoring. Welk aandeel van deze hogescholen de software Proctorio gebruikt, wordt niet actief gemonitord.

Vraag 5
Hoe zijn studenten die Proctorio van de onderwijsinstelling hebben moeten installeren op de hoogte gebracht van het lek?

Antwoord 5
Onderwijsinstellingen communiceren via hun interne kanalen over (het gebruik van) Proctorio. Denk hierbij aan nieuwsberichten of Q&A's. Wat betreft het beveiligingslek geldt dat er ondanks het lek, voor zover bekend, geen gegevens gelekt of gestolen zijn.

Vraag 6
Welke maatregelen hebben instellingen die Proctorio verplichtten genomen, nadat bekend is geworden dat de software onveilig is?

Antwoord 6
Onderwijsinstellingen zijn nagegaan of het gevonden lek bij Proctorio gedicht is. Proctorio heeft aangegeven dat het lek binnen een week gedicht is.

Vraag 7
Welke andere antispieksoftware wordt op dit moment gebruikt door hogeronderwijsinstellingen en hoe wordt gecontroleerd of die wel veilig genoeg is?

Antwoord 7
Onderwijsinstellingen maken gebruik van verschillende proctoring software. Voorbeelden hiervan zijn *Proctorio*, *Proctorexam* en *Proctor-u*. Onderwijsinstellingen zijn verantwoordelijk voor een veilige werk- en leeromgeving.

---

[2] https://www.rijksoverheid.nl/documenten/publicaties/2020/07/10/servicedocument-ho---aanpak-coronavirus-covid-19
[3] aanbevelingen_online_proctoring_onderwijs.pdf (autoriteitpersoonsgegevens.nl)
[4] surf-rapport-online-proctoring_2020_update-april-2020.pdf

Daarom gaan zij onder andere via risicoanalyses, pentesten en afspraken over security audits en *Data Protection Impact Assessment* (DPIA) na of de software veilig is. Daarnaast trekken de onderwijsinstellingen samen met SURF op om gezamenlijk eisen te stellen aan alle proctoring software.

Vraag 8
Aan welke privacy-eisen moeten hogeronderwijsinstellingen voldoen voor het gebruiken van antispieksoftware?

Antwoord 8
Hoger onderwijsinstellingen moeten altijd voldoen aan privacyregelgeving. In het kader van de inzet van online proctoring heeft de Autoriteit Persoonsgegevens aanbevelingen gepubliceerd op 2 oktober 2020 in het document «Aanbevelingen online proctoring onderwijs». Hierin staat onder andere dat online proctoring alleen wordt ingezet als het noodzakelijk is en de privacyinbreuk moet zo klein mogelijk zijn. Voor online proctoring vindt de Autoriteit Persoonsgegevens het van belang dat onderwijsinstellingen instellingsbrede afspraken of richtlijnen opstellen voor het beschermen van de privacy.
De *Whitepaper online proctoring: surveilleren op afstand*(april 2020) van SURF kan hoger onderwijsinstellingen ook helpen bij de keuze van het wel of niet inzetten van antispieksoftware.[5]

Vraag 9
Hoe wilt u de privacy van studenten en medewerkers in de toekomst garanderen nu steeds meer toepassingen in het onderwijs digitaal zijn en geleverd worden door commerciële partijen?

Antwoord 9
Onderwijsinnovatie door middel van digitalisering kan bijdragen aan kwalitatief goed en flexibeler onderwijs. Onderwijsinstellingen willen daarom de kansen die digitalisering biedt, benutten voor beter onderwijs. Ik ondersteun dat. Maar digitalisering brengt ook uitdagingen met zich mee. Onderwijsinstellingen kunnen online kwetsbaar zijn. Gegevens van bijvoorbeeld studenten en medewerkers dienen goed beschermd te zijn. Onderwijsinstellingen en commerciële aanbieders van software dienen zich altijd te houden aan privacyregelgeving en zijn verantwoordelijk voor de privacy van studenten en medewerkers. Daar krijgen onderwijsinstellingen ondersteuning bij van SURF. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van privacyregelgeving. OCW is en blijft in gesprek met de koepels over het thema privacy. In specifieke gevallen kan OCW optreden zoals gebeurde in de gezamenlijke *Data Protection Impact Assessment*(DPIA) inzake Google.

Vraag 10
Kunt u in kaart brengen welke andere privacyrisico's studenten en medewerkers nu lopen?

Antwoord 10
Het is de verantwoordelijkheid van hoger onderwijsinstellingen om de privacy op orde te hebben. Daarover leggen hoger onderwijsinstellingen geen verantwoording af bij OCW.

Vraag 11 en 12
Bent u voornemens om aanvullende protocollen op te stellen voor het gebruik van antispieksoftware, zoals instemmingsrecht van de medezeggenschap?
Hoe kijkt u, tegen deze achtergrond, terug op uw antwoorden op eerdere Kamervragen waarin u aangaf dat instellingen zelf mogen bepalen of de medezeggenschap meebeslist over online proctoring?[6]

---

[5] Whitepaper online proctoring: surveilleren op afstand | SURF.nl
[6] Aanhangsel van de Handelingen II, 2020–2021, nr. 3241

Antwoord 11 en 12
Antispieksoftware wordt door het hoger onderwijs gebruikt om fraude te voorkomen. Fraudebestrijding is niet onderhevig aan wettelijk instemmingsrecht van de medezeggenschap. Er is geen voornemen om daar iets aan te wijzigen in de wet. Dit neemt niet weg dat zorgvuldig moet worden omgegaan met het gebruik van antispieksoftware met inachtneming van privacyregelgeving. De medezeggenschap kan desgewenst proactief het gesprek aangaan met het bestuur. Ik moedig de studenten en onderwijsinstellingen nog steeds aan om regelmatig in dialoog te gaan over dit onderwerp.
In mijn antwoord op vraag 3 benoemde ik al dat de Autoriteit Persoonsgegevens aanbevelingen heeft gegeven aan instellingen over het omgaan met antispieksoftware. Ook refereerde ik aan het Whitepaper over antispieksoftware van SURF. Er is geen aanleiding voor mij om hiernaast nog aanvullende protocollen op te stellen.