Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

4015

Vragen van het lid **Wiersma** (VVD) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het bericht «Gegevens van alumni, donateurs en relaties Universiteit Utrecht in handen van hackers»* (ingezonden 14 augustus 2020).

Antwoord van Minister **Van Engelshoven** (Onderwijs, Cultuur en Wetenschap) (ontvangen 7 september 2020).

Vraag 1
Bent u bekend met het data-veiligheidsincident bij leverancier Blackbaud, waar in ieder geval alumni, donateurs en relaties van Universiteit Utrecht en TU Delft door zijn getroffen?[1, 2]

Antwoord 1
Ja.

Vraag 2 t/m 7
Welke gegevens zijn er precies buitgemaakt bij de datalek die veroorzaakt is door de aanval op Blackbaud? Op welke manier hebben Universiteit Utrecht en TU Delft inmiddels de gedupeerden geïnformeerd over het datalek, waardoor gegevens van alumni, donateurs en relaties op straat zijn komen te liggen?
Welke garantie hebben Universiteit Utrecht en TU Delft gekregen dat de buitgemaakte gegevens daadwerkelijk zijn vernietigd, nadat Blackbaud losgeld heeft betaald aan de internetcriminelen? Op welke manier kunnen de getroffen alumni, donateurs en relaties dit controleren?
Waarop baseert de Universiteit Utrecht «de schatting van de waarschijnlijkheid van eventuele risico's voor de privacy van betrokkenen momenteel in als laag»?[3] Is het niet zo dat door de aanval privacygevoelige data al lang op straat liggen, dus dat lage schatting van de risico's nergens op gebaseerd is?

---

[1] Gegevens van alumni, donateurs en relaties Universiteit Utrecht in handen van hackers, RTV Utrecht, 11 augustus 2020 (https://www.rtvutrecht.nl/nieuws/2085024/)

[2] Universiteit Utrecht, 11 augustus 2020, data veiligheidsincident bij leverancier blackbaud (https://www.uu.nl/nieuws/data-veiligheidsincident-bij-leverancier-blackbaud) en TU Delft, 11 augustus 2020 (https://www.tudelft.nl/2020/alumni/cyberaanval-op-blackbaud/)

[3] Privégegevens afgestudeerden TU Delft en Universiteit Utrecht gestolen, security.nl, 11 augustus 2020 (https://www.security.nl/posting/667321/Priv%C3%A9gegevens+afgestudeerden+TU+Delft+en+Universiteit+Utrecht+gestolen)

ah-tk-20192020-4015
ISSN 0921 - 7398
's-Gravenhage 2020

Klopt het dat op 17 juli 2020 de datadiefstal al bekend was en dat op 24 juli meer dan 20 Britse universiteiten al op de hoogte waren van het datalek? Waarom werden Nederlandse universiteiten pas op 11 augustus 2020 hierover geïnformeerd?
Hoe kan het dat aanvallers toegang kregen tot een oude back-up uit 2017 die nog in de omgeving van Blackbaud stond? Op welke manier controleren hoger onderwijsinstellingen of bepaalde privacygevoelige gegevens daadwerkelijk nog in het bezit zijn van derde partijen?
Wie is uiteindelijk eindverantwoordelijk voor het goed verwerken en beveiligen van privacygegevens van alumni, donateurs en relaties? Is dat de hoger onderwijsinstelling of een derde partij zoals een cloud softwarebedrijf? Indien de hoger onderwijsinstelling, hoe kan het dat Blackbaud nog beschikte over een oude back-up uit 2017?

Antwoord 2 t/m 7
Het is de verantwoordelijkheid van de hoger onderwijsinstellingen zorg te dragen voor de opslag en verwerking van gegevens van studenten, medewerkers, alumni en overige personen die informatie aan de instelling hebben verstrekt. Daartoe behoort ook het inrichten van de informatiesystemen op een zodanige wijze dat deze veilig zijn voor inbreuken («hacks»). In mijn brieven van 14 februari 2020 inzake cyberveiligheid in het onderwijs en van 3 juli 2020 inzake het onderzoek naar de cyberaanval op de Universiteit Maastricht heb ik uiteengezet welke maatregelen hoger onderwijsinstellingen hebben genomen om de cyberveiligheid te vergroten. Deze maatregelen betreffen een breed spectrum: het gaat zowel om het vergroten van het veiligheidsbewustzijn bij alle betrokken partijen, als om het verbeteren van detectie en het toedelen van de verantwoordelijkheid op de juiste niveaus binnen de instelling.
Ik heb daarbij aangegeven dat 100% veiligheid niet bestaat; hoger onderwijsinstellingen zijn door hun open en transparante karakter kwetsbaar. Instellingen moeten streven naar een integrale veiligheidsaanpak waarin een afweging wordt gemaakt tussen kernwaarden als openheid, te beschermen belangen zoals de bescherming van persoonsgegevens en bedreigingen.

Vraag 8 en 9
Op welke manier gaat u erop toezien dat hoger onderwijsinstellingen beter controleren op welke manier derde partijen omgaan met privacygevoelige informatie? En welke maatregelen gaat u specifiek treffen om een herhaling van dit incident te voorkomen?
Kunt u specifiek toelichten in welke mate u de online veiligheid van privacygevoelige informatie onder de verantwoordelijkheid van het Ministerie van Onderwijs Cultuur en Wetenschap vindt vallen en of de verschillende cyberaanvallen van de afgelopen tijd naar uw mening vragen om bijstelling van deze verantwoordelijkheid?

Antwoord 8 en 9
In mijn brief van 3 juli 2020 inzake het onderzoek naar de cyberaanval op de Universiteit Maastricht heb ik uw Kamer laten weten dat de Inspectie van het Onderwijs een onderzoek uitvoert naar de cyberveiligheid op stelselniveau. Ik heb daarbij het belang van ketensamenwerking en transparantie tussen de instellingen onderling en andere ketenpartners met daar waar nodig de hulp van de overheid als stelselverantwoordelijke onderstreept. Ook heb ik toegezegd uw Kamer daarover begin volgend jaar te informeren. In mijn reactie op het onderzoek van de inspectie zal ik nader ingaan op de verantwoordelijkheidsverdeling rondom cyberveiligheid.