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

575

Vragen van de leden **Van der Woude** en **Rajkowski** (beiden VVD) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het bericht «Psychische problemen HAN-studenten ook op straat na grote hack»* (ingezonden 7 oktober 2021).

Antwoord van Minister **Van Engelshoven** (Onderwijs, Cultuur en Wetenschap) (ontvangen 4 november 2021).

Vraag 1
Bent u bekend met het bericht «Psychische problemen HAN-studenten ook op straat na grote hack»?[1]

Antwoord 1
Ja.

Vraag 2
Is het waar dat de hogeschool van Arnhem en Nijmegen (HAN) vorige maand is aangevallen met gijzelsoftware? Zo ja, kunt u een chronologisch feitenrelaas schetsen van deze gebeurtenis en kunt u hierbij specifiek ingaan op de oorzaak van de cyberaanval? Zo nee, waarom niet? Deelt u de mening dat het wenselijk is om de kennis over het ontstaan van hack te delen met andere onderwijsinstellingen zodat zij hier lering uit kunnen trekken?

Antwoord 2
De HAN University of Applied Sciences (HAN) is geconfronteerd met een hack. De HAN heeft mij laten weten dat een hacker via een webformulier toegang heeft gekregen tot een server van de HAN waarop veel gegevens stonden. Van gijzelsoftware is in dit geval géén sprake. Voor een chronologisch feitenrelaas verwijs ik naar de website van de HAN, www.han.nl/datalek waar via een liveblog de ontwikkelingen in de tijd te volgen zijn. Het is van groot belang om de kennis over het ontstaan van hacks te delen met andere onderwijsinstellingen, aangezien voor een effectieve bestrijding van cyberrisico's samenwerking en continue kennis-en informatiedeling cruciaal is. Dat is ook in dit geval gebeurd. Zie ook het antwoord op vraag 5.

[1] RTL Nieuws, 05/10/2021; https://www.rtlnieuws.nl/nieuws/nederland/artikel/5258411/han-hack-datalek-psychische-problemen-medische-informatie

ah-tk-20212022-575
ISSN 0921 - 7398
's-Gravenhage 2021

Vraag 3
Is het waar dat bij deze hack zeer gevoelige gegevens zoals medische en persoonsgegevens van studenten van de HAN buit zijn gemaakt als gevolg van de cyberaanval? Zo ja, kunt u een overzicht geven van de omvang van deze gegevens en welke gegevens precies buit zijn gemaakt? Zo nee, waarom niet?

Antwoord 3
De HAN heeft mij laten weten dat de hacker toegang heeft gehad tot een omgeving waar veel persoonsgegevens beschikbaar waren en heeft op 5 oktober een overzicht van de gelekte data gepubliceerd op haar website han.nl/datalek. Dit overzicht is als bijlage toegevoegd aan een persbericht dat op dezelfde dag is verschenen. Uit het overzicht blijkt dat het in 95% van de gevallen gaat om algemene persoonsgegevens zoals adresgegevens of telefoonnummers. Van een klein percentage van de mogelijk getroffen gegevens (3%) gaat het om meer persoonlijke gegevens waaronder informatie over de reden van studievertraging of bijzondere omstandigheden waar de hogeschool rekening mee wil houden.

Vraag 4
Is de datadiefstal reeds gemeld bij de Autoriteit Persoonsgegevens (AP)? Zo ja, is er verder contact geweest tussen de HAN en de AP? Zo nee, waarom niet?

Antwoord 4
Ja. De HAN heeft zodra zij weet had van het datalek direct de AP geïnformeerd. Deze (voorlopige) melding is op 1 september door de Functionaris Gegevensbescherming van de HAN gedaan. Zodra er nieuwe ontwikkelingen waren en de voorlopige melding kon worden aangevuld is de AP daarvan steeds op de hoogte gebracht.

Vraag 5
Heeft de HAN ten tijde van de aanval met gijzelsoftware in contact gestaan met het sectorale computer emergency response team SURFcert ter (technische) ondersteuning? Zo ja, heeft de HAN dit contact geïnitieerd? Zo ja, wat is er uit dit contact gekomen qua ondersteuning vanuit SURFcert?

Antwoord 5
De HAN heeft mij laten weten dat er van gijzelsoftware géén sprake is geweest (zie vraag 2). Zodra de HAN weet had van het datalek heeft de HAN op 1 september contact gezocht met SURFcert. SURFcert heeft de HAN ondersteund met het analyseren van het incident. De Indicators of Compromise (IOCs) zijn daarbij gedeeld met het SURFcert en de daarbij aangesloten instellingen.

Vraag 6
Is er een dialoog geweest tussen de HAN en de hacker in kwestie over het wel of niet betalen van het geëiste losgeld bedrag? Zo ja, heeft de HAN de politie ingeschakeld bij het voeren van deze dialoog? Zo nee, waarom niet?

Antwoord 6
De HAN heeft mij laten weten dat er contact is geweest met de hacker. De HAN is niet ingegaan op de eisen van het losgeld. Zodra de HAN kennis had van het datalek heeft zij direct contact gezocht met de politie en ook aangifte gedaan.

Vraag 7
Is het waar dat de gestolen data zijn gepubliceerd? Zo ja, waar en zijn de studenten en medewerkers hiervan op de hoogte gesteld? Zo nee, waarom niet?

Antwoord 7
Voor zover bekend zijn er geen data gepubliceerd. Omdat niet bekend is welke data er exact zijn buitgemaakt heeft de HAN vanuit het oogpunt van zorgvuldigheid en voorzorg besloten om iedereen van wie mogelijk persoonsgegevens zijn buitgemaakt te informeren.

Vraag 8
Kunt u een inschatting maken van de (immateriële) schade en kosten die deze cyberaanval tot nu heeft veroorzaakt?

Antwoord 8
Deze inschatting is vooralsnog niet te geven. De werkzaamheden bij de HAN lopen nog door. Hier zijn naast eigen medewerkers ook externe deskundigen bij betrokken.

Vraag 9
Is het waar dat de HAN een «makkelijk doelwit» is genoemd door de hacker in kwestie? Zo ja, hoe beoordeelt u deze uitspraak? Deelt u de mening dat het zeer zorgelijk is dat een Nederlandse hoger onderwijsinstelling op deze wijze wordt bestempeld door cybercriminelen?

Antwoord 9
De uitspraak van de hacker is opgetekend door een journalist. Ik kan daarover niet oordelen. De HAN heeft in haar bedrijfsvoering veel aandacht voor IT veiligheid. Dat blijkt onder andere uit de aanwezigheid van diverse preventieve, detectieve, responsieve en correctieve maatregelen. Voorbeelden daarvan zijn de regelmatige uitvoering van penetratietesten o.a. door ethical hackers, de aansluiting op de Security Operations Center oplossing geboden door het SURFsoc en de aanwezigheid van offline back-up faciliteiten. Daarnaast wordt met enige regelmaat het bewustzijn van medewerkers en studenten rond informatiebeveiliging verhoogd middels campagnes. Ook is deelgenomen aan de landelijke OZON-oefening van SURF op 18 maart jl. Middels de planning & control cyclus wordt invulling gegeven aan de verdere groei in volwassenheid op het gebied van informatiebeveiliging, om zo in te kunnen spelen op het continu veranderde cyberdreigingslandschap waar de onderwijssector mee te maken heeft.

Vraag 10
Deelt u de mening dat deze cyberaanval en in het bijzonder het buit maken van gevoelige medische gegevens van ruim 2000 studenten een zeer grote inbreuk maakt op de privacy van de studenten in kwestie? Deelt u de mening dat het voor studenten die slachtoffer zijn geworden, wenselijk is om ondersteuning te krijgen over eventuele gevaren met betrekking tot identiteitsfraude en hoe om te gaan met een eventuele psychische impact die bij het prijsgegeven van dit type gevoelige gegevens komt kijken, bijvoorbeeld van de Fraudehelpdesk? Zo ja, kunt u dit meegeven aan het bestuur van de HAN? Zo nee, waarom niet?

Antwoord 10
Persoonsgegevens en bijzondere persoonsgegevens worden beschermd via de daarvoor geldende wetgeving (AVG). Dat er gegevens van medische aard betrokken zijn bij het datalek is uiteraard bijzonder te betreuren. De HAN heeft alle mogelijk getroffen personen van het datalek geïnformeerd, waarbij de personen van wie mogelijk gevoelige gegevens zijn betrokken als eerste zijn geïnformeerd. Een team van professionals heeft vanaf het moment van informeren klaargestaan om eventuele vragen te beantwoorden. Wanneer op basis van reacties het vermoeden bestaat dat er extra nazorg nodig is, worden mensen gewezen op de diverse voorzieningen die de HAN heeft op dit gebied zoals studentpsychologen. Ook monitort de HAN of de verdere opvolging wellicht bijsturing behoeft.

Vraag 11
Deelt u de mening dat onderwijsinstellingen meer moeten doen om dergelijke cyberaanvallen te voorkomen? Zo ja, deelt u dan ook de mening dat bijvoorbeeld moet worden gekeken naar minimale beveiligeisen om de digitale hygiëne op orde te krijgen? Zo ja, hoe komt dit overeen met uw eerdere uitspraken dat de verantwoordelijkheid van goede bedrijfsvoering bij de instelling zelf ligt en ze in beginsel dus zelf verantwoordelijkheid zijn om de eigen kwetsbaarheden in de cyberveiligheid te mitigeren? Zo nee, waarom niet?

Antwoord 11
Hogescholen hebben afgelopen jaren op grond van toenemende dreiging hun aanpak geïntensiveerd. De hack bij de Universiteit Maastricht, maar ook andere incidenten, heeft de sector doen beseffen hoe belangrijk digitale veiligheid en een goede voorbereiding is. In mijn brief van 28 september jl. heb ik uiteengezet welke maatregelen de sector en ik reeds getroffen hebben en welke op stapel staan. [2]

Vraag 12
Kunt u bovenstaande vragen voor het nog in te plannen commissiedebat «Digitalisering in het onderwijs» beantwoorden?

Antwoord 12
Ja.

[2] Kamerstuk «Digitale weerbaarheid in het hoger onderwijs en onderzoek en in het middelbaar beroepsonderwijs | 28-09-2021.