Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

## 797

Vragen van de leden **Raemakers** (D66), **Hijink** (SP) en **Wörsdörfer** (VVD) aan de Staatssecretaris van Volksgezondheid, Welzijn en Sport over *wederom een datalek in de jeugdzorg* (ingezonden 8 oktober 2020).

Antwoord van Staatssecretaris **Blokhuis** (Volksgezondheid, Welzijn en Sport) (ontvangen 16 november 2020).

Vraag 1
Bent u bekend met het artikel «Groot datalek bij Jeugdriagg: medische dossiers kwetsbare kinderen gelekt»?[1]

Antwoord 1
Ja.

Vraag 2
Had dit specifieke datalek volgens u voorkomen kunnen worden, kijkend naar een eerder datalek in april 2019 en het recent uitgebrachte rapport van de IGJ «Extra aandacht nodig voor ICT in de jeugdzorg»?[2] [3]

Antwoord 2
Het datalek bij Kenter is op een vergelijkbare wijze ontstaan als een eerder datalek in april 2019. Dat het weer mogelijk was om op vergelijkbare wijze toegang tot persoonsgegevens te krijgen is zorgelijk. Naar aanleiding van het datalek in 2019 bij SAVE Utrecht heeft Z-CERT een domein naam check gedaan en JZNL heeft jeugdhulpaanbieders opgeroepen zelf een check te doen op oude domeinnamen. De oude domeinnamen van Kenter waren in 2015 voor 5 jaar afgekocht en verliepen op 1 januari 2020 en ontliepen daarmee onder andere de Z-CERT check in 2019. Het niet afsluiten van een oude domein naam kan eenvoudig worden voorkomen.

[1] RTL Nieuws, 1 oktober 2020 (https://www.rtlnieuws.nl/nieuws/nederland/artikel/5187220/jeugdriagg-kenter-jeugdhulp-datalek-dossiers)
[2] https://www.rtlnieuws.nl/tech/artikel/4672826/jeugdzorg-datalek-dossiers-kinderen-utrecht-email
[3] Inspectie Gezondheidszorg en Jeugd – Extra aandacht nodig voor ICT in de jeugdzorg – juni 2020

ah-tk-20202021-797
ISSN 0921 - 7398
's-Gravenhage 2020

Vraag 3
Hoe is de aangenomen motie van de leden Raemakers en Hijink van 2 juli 2020 uitgevoerd waarin de regering verzocht wordt om met branches in gesprek te gaan over ICT-problemen in de jeugdzorg om jeugdzorgorganisaties uiterlijk 1 oktober te helpen met het beveiligen van de aan hen toevertrouwde data van jongeren en hun ouders?[4]

Antwoord 3
Naar aanleiding van de motie Raemakers en Hijink uit 2019 en 2020 zijn gesprekken gevoerd met Jeugdzorg Nederland en Z-CERT. In samenwerking met Jeugdzorg Nederland is Deloitte in staat gesteld penetratietesten uit te voeren. Daarnaast heeft Jeugdzorg Nederland zijn achterban geïnformeerd over het risico van niet goed afgesloten domeinnamen. De in de BGZJ verzamelde branches hebben dit in een breder kader gedaan. Naar aanleiding van de pentesten uit 2019 hebben de zes gepenteste aanbieders hun beleid aangepast. Op basis van de genomen maatregelen wordt een handreiking geschreven, met aandacht voor de implementatie van de wettelijk verplichte NEN 7510 norm, die in december 2020 wordt verwacht, waarna deze nog beter kan worden geïmplementeerd.

Vraag 4
Wanneer wordt jeugdzorgaanbieders eindelijk de mogelijkheid geboden om zich aan te sluiten bij Z-CERT conform de aangenomen motie-Raemakers en Hijink van 25 juni 2019, aangezien Z-CERT in het genoemde artikel meldt dat de meeste incidenten nog steeds plaatsvinden omdat de basis niet op orde is?[5]

Antwoord 4
Datalekken hebben vaak een systeem- en een menselijke component. Voor de systeem component kan Z-CERT, als de ICT brandweer, ondersteuning bieden bij een crisis en informatie delen en ter voorkoming van cyber incidenten informatie delen over relevante dreigingen en kwetsbaarheden van gebruikte systemen inzake dataveiligheid. Z-CERT is dan ook binnen deze context in gesprek met Jeugdzorg Nederland over wat zij voor elkaar kunnen betekenen. Door de risico gestuurde aanpak van Z-CERT gaan we opnieuw de mogelijkheden voor aansluiting onderzoeken. De aansluiting van Jeugdhulpaanbieders op Z-Cert kan dan op zijn vroegst in Q1 van 2021 starten.

Vraag 5
Kijkt u nu anders naar de rol van het Ministerie van VWS als het gaat om het beter beveiligen van gegevens in de jeugdzorg?

Antwoord 5
Het Ministerie van VWS draagt ketenverantwoordelijkheid voor de dataveiligheid in het jeugddomein. Jeugdhulpaanbieders dragen echter zelf de verantwoordelijkheid voor het op orde houden van hun eigen dataveiligheid, ook indien er sprake is van een fusie en/of naamswijziging. Zodoende vragen wij de branches Jeugdzorg Nederland, VGN en GGZ-Nederland een voortrekkersrol te spelen op het gebied van informatiebeveiliging. Voor dataveiligheid zijn door het Rijk als ketenverantwoordelijke regels gesteld, zoals de wettelijk verplichte NEN 7510 norm. Bovendien zijn er toezichthouders, zoals de AP en de IGJ. Alle jeugdhulporganisaties dienen aan deze wettelijke vereisten te voldoen.

Vraag 6
Hoeveel pentesten zijn er afgelopen half jaar gedaan door het Ministerie van VWS en hoeveel worden er de komende periode uitgevoerd?

Antwoord 6
In 2019 zijn er bij zes jeugdhulpaanbieders en Gecertificeerde Instellingen pentesten uitgevoerd en voor 2021 worden deze pentesten bij zes andere jeugdhulporganisaties uitgevoerd. De testen hebben plaatsgevonden bij grote

[4] Kamerstuk 31 839, nr. 737
[5] Kamerstuk 31 839, nr. 676

jeugdhulporganisaties, omdat een datalek daar een impact zou kunnen hebben op een groot aantal cliënten.

Vraag 7
Welke regels zijn er ten aanzien van ethisch hacken door derden, zoals journalisten, omdat hierbij inzage is in privacygevoelige gegevens?

Antwoord 7
Met het oog op het verminderen van kwetsbaarheden in ICT-systemen heeft het Nationaal Cyber Security Centrum (NCSC) een Leidraad Coordinated Vulnerability Disclosure (CVD) opgesteld.[6] Veel grotere Nederlandse organisaties hebben een eigen CVD gedragscode opgesteld en gepubliceerd op hun website. De organisatie geeft hiermee aan dat het is toegestaan – onder bepaalde randvoorwaarden – om de beveiliging van de ICT systemen van de organisatie ongevraagd te onderzoeken op mogelijke beveiligingsissues zonder dat er aangifte wordt gedaan. Als een ethische hacker zich houdt aan de gedragscode, zoals het niet publiceren van ingeziene data, zal de organisatie geen aangifte doen van computervredebreuk. Het vinden van kwetsbaarheden kan niettemin gepaard gaan met het overtreden van de wet. Als er aangifte wordt gedaan, is in Nederland het bestaan en naleven van CVD-beleid een relevante omstandigheid die de officier van justitie zal meenemen in zijn beslissing om al dan niet een strafrechtelijk onderzoek in te laten stellen en/of te vervolgen.

Vraag 8
Kunt u deze vragen afzonderlijk en ruim voor het wetgevingsoverleg Jeugd van 23 november 2020 beantwoorden?

Antwoord 8
Ja.

[6] De Leidraad Coordinated Vulnerability Disclosure is een herziening van de eerdere leidraad «Responsible Disclosure».