Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

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

329

Vragen van de leden **Rahimi** en **Rajkowski** (beiden VVD) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid over *het bericht «Experts sabelen overheid neer om belangrijke websites als DigiD: «Pas nu domeinnaam aan»»* (ingezonden 4 oktober 2023).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) mede namens de Minister van Justitie en Veiligheid (ontvangen 30 oktober 2023).

Vraag 1
Bent u bekend met het bericht «Experts sabelen overheid neer om belangrijke websites als DigiD: «Pas nu domeinnaam aan»»?[1]

Antwoord 1
Ja.

Vraag 2 en 3
Deelt u de mening dat het gebruik van topleveldomeinnamen, zoals ook gevraagd tijdens het commissiedebat Digitaliserende overheid d.d. 28 juni jl. een goed idee is en wat is de status hiervan[2]?
Zo ja, op welke termijn verwacht u dit door te kunnen voeren?

Antwoord 2 en 3
Zoals opgenomen in de Werkagenda Waardengedreven Digitaliseren[3], heb ik onder de pijler 2: Iedereen kan de digitale wereld vertrouwen, opgenomen te komen tot de invoering van een second-level-domein (SLD) voor de overheid. Als voorbeeld is in de Werkagenda opgenomen de SLD overheid.nl, daarnaast wordt ook gov.nl overwogen.
Met de toename van domeinnamen van de overheid is de herkenbaarheid van overheidswebsites in het geding gekomen. Een eigen topleveldomeinnaam (TLD) zoals bijvoorbeeld .gov, .overheid of .nld is nu niet mogelijk. De

[1] AD, 2023. Experts sabelen overheid neer om belangrijke websites als DigiD: «Pas nu domeinnaam aan» https://www.ad.nl/tech/experts-sabelen-overheid-neer-om-belangrijke-websites-als-digid-pas-nu-domeinnaam-aan~ad983c05/.
[2] Zie ook de toezegging aan het lid Rahimi (VVD) tijdens het commissiedebat Digitaliserende overheid van 28 juni 2023. TZ202307–069.
[3] Werkagenda Waardengedreven Digitaliseren – Digitale Overheid.

ah-tk-20232024-329
ISSN 0921 - 7398
's-Gravenhage 2023

TLD .gov is al in bezit van de Amerikaanse overheid en kan dus niet gebruikt worden door de Nederlandse overheid.
In 2012, tijdens de laatste uitbreiding van TLD's heeft de Internet Corporation for Assigned Names and Numbers (ICANN), de organisatie waar je een TLD moet aanvragen, de regel gehandhaafd dat 3 letterige ISO country codes TLD (ccTLD) zoals .nld niet uitgegeven worden.[4] Nederland gebruikt op dit moment de 2 letterige ccTLD .nl en het huidige .nl domein werkt goed [zie Kamerstuk 26 643, nr. 947]. ICANN zal de regel over niet toekennen van 3 letterige ccTLD zeer waarschijnlijk ook handhaven in de volgende uitbreidingsronde van TLD door ICANN. Verwacht wordt dat ICANN waarschijnlijk in 2026 de aanmelding voor een volgende uitbreidingsronde voor TLD's opent. Tot die tijd zou Nederland geen aanvraag voor een TLD kunnen indienen.
Veel landen hanteren specifiek voor overheidswebsites de SLD extensie .gov zoals het Verenigd Koninkrijk (gov.uk), Tsjechië (gov.cz), Polen (gov.pl), Griekenland (gov.gr) en Portugal (gov.pt). Het is inmiddels een internationale standaard voor overheidswebsites én herkenbaar, korter en daardoor ook veiliger. Uit recent onderzoek[5] van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) blijkt aantoonbaar dat een uniforme extensie burgers helpt te bepalen of een website van de overheid is of niet.
Momenteel wordt gewerkt aan een implementatie-aanpak voor één extensie. Over de gemaakte keuze en aanpak wil ik uw Kamer via de Voortgangsrapportage van de Werkagenda Waardengedreven Digitaliseren eind dit jaar nader informeren. Voor de daadwerkelijke implementatie zal er vervolgens enige tijd nodig zijn; dit zal nader toegelicht worden in de implementatie-aanpak.

Vraag 4
Waarom hebben namen van websites als DigiD en andere websites van de overheid (nog) geen specifieke domeinnamen?

Antwoord 4
Overheden zijn nu vrij domeinnamen voor hun websites te kiezen. Voor Rijksoverheden wordt deze vrijheid begrensd door de afspraken die zijn vastgelegd in het Domeinnaambeleid Rijksoverheid.[6] De afspraken bevatten onder meer criteria voor het gebruik van topleveldomeinen door de Rijksoverheid zoals .nl, .eu, .com, .aw-, .cw- en .sx. En verder zijn er afspraken dat overige TLD's zoals bijvoorbeeld .nu, .org, .net, .gov, .info, .biz, .mil niet gebruikt worden voor Nederlandse Rijksoverheidsdoeleinden.

Vraag 5
Hoe beoordeelt u dat er wordt gesteld dat de overheid domeinnamen van de eigen websites zo snel mogelijk moet aanpassen naar .gov of .overheid om de opmars van cybercriminaliteit de pas af te snijden?

Antwoord 5
De invoering van een uniform domeinnaamachtervoegsel zal de herkenbaarheid van de overheid online vergroten, zoals ik ook vermeldde in de «Werkagenda Waardengedreven Digitaliseren» die ik eind 2022 met u deelde. Het is echter geen middel om cybercriminaliteit met online overheidsdiensten volledig te voorkomen.
Zoals toegelicht in vraag 2 is de invoering van een top-level domeinnaam (TLD) voor de overheid nu niet mogelijk. De second-level domeinnamen (SLD) overheid.nl en gov.nl zijn al in bezit van de Nederlandse overheid. Deze domeinnamen kunnen als uniform achtervoegsel (ook wel suffix of extensie genoemd) worden gebruikt voor domeinnamen van de overheid. Daaronder kunnen dan domeinnamen voor organisaties worden geregistreerd zoals bijv. minbzk.overheid.nl of minbzk.gov.nl. Verschillende andere landen hanteren al een vergelijkbare aanpak of werken aan de invoering ervan, zoals Groot-Brittannië (gov.uk), Tsjechië (gov.cz), Griekeland (gov.gr), Polen (gov.pl) en

[4] https://newgtlds.icann.org/sites/default/files/guidebook-full-04jun12-en.pdf.
[5] Onderzoek domeinnaamextensie (digitaleoverheid.nl).
[6] Domeinnaambeleid | Rijkswebsites | CommunicatieRijk.

Portugal (gov.pt). Ik ben voorstander van het invoeren van een SLD-extensie en zal me daarvoor ook blijven inzetten, maar een volledige overstap zal tijd kosten.

Vraag 6
Deelt u de mening dat er spoedig specifieke domeinnamen moeten komen voor de hiervoor genoemde websites? Zo neen, waarom niet?

Antwoord 6
Ik vind het belangrijk dat de digitale overheid herkenbaar en veilig is voor burgers en uit recent burgeronderzoek[7] is gebleken dat één uniforme domeinnaamextensie zoals bijvoorbeeld overheid.nl of gov.nl bijdraagt aan de herkenbaarheid van de overheid. Een dergelijk extensie kan, na invoering, ook worden toegepast op websites zoals DigiD.

Vraag 7
Bent u voornemens de domeinnamen spoedig te veranderen? Zo neen, waarom niet? Zo ja, wanneer zou dat gerealiseerd kunnen zijn?

Antwoord 7
Op dit moment werkt het Ministerie van BZK interdepartementaal de mogelijkheid uit om één uniforme domeinnaamextensie voor alle publieksgerichte websites van de overheid in te voeren. Dat zal gebaseerd zijn op een SLD zoals overheid.nl of gov.nl. Ook is het Nationaal Cyber Security Centrum gevraagd een advies uit te brengen over welk extensiegebruik (gov.nl of overheid.nl) vanuit digitale veiligheid de voorkeur geniet.
Verder is begin oktober het Register van Overheidsorganisaties (ROO) uitgebreid met de bèta-versie van het Register Internetdomeinen Overheid (RIO).[8] In het register staan alle publieke domeinen en -registraties van de Rijksoverheid opgenomen. Aan de hand van het register kunnen burgers nu al controleren of een domeinnaam die men bezoekt bij de overheidsorganisatie hoort die wordt verwacht. Vanaf begin 2024 worden ook de domeinen van andere overheden in het register vindbaar en zal meer bekendheid gegeven worden aan het RIO.

Vraag 8
Wanneer kan de voortgangsrapportage integrale aanpak onlinefraude worden verwacht, die zoals toegezegd tijdens het commissiedebat Cybercrime d.d. 30 maart jl.[9], informatie bevat over de pilot gegevensuitwisseling, gezien banken, politie en het OM informatie hebben die helaas nog te weinig bij elkaar wordt gebracht, waardoor cybercriminelen vrij spel lijken te hebben?

Antwoord 8
De Minister van Justitie en Veiligheid zendt u uiterlijk begin 2024 de toegezegde voortgangsrapportage over 2023.

Vraag 9
In het debat Online veiligheid en cybersecurity van 29 juni 2023 is toegezegd[10] om informatie over terugvalopties en de hele weerbaarheidsanalyse terug te laten komen in de update van de versterkte aanpak bescherming vitale infrastructuur: hoe staat het met de uitwerking van deze toezegging?

Antwoord 9
Uw Kamer wordt voor het einde van dit jaar door de Minister van Justitie en Veiligheid geïnformeerd over deze toezegging en over de motie Rajkowski en Van Raan over het in kaart brengen in hoeverre terugvalopties nodig zijn voor het versterken van de digitale weerbaarheid (26 643 nr. 1053).

---

[7] Onderzoek domeinnaamextensie (digitaleoverheid.nl).
[8] Register Internetdomeinen Overheid.
[9] Toezegging aan het lid Rajkowski (VVD) tijdens het commissiedebat Cybercrime d.d. 30 maart 2023. TZ202303–121.
[10] Toezegging aan het lid Rajkowski (VVD) tijdens het commissiedebat Online veiligheid en cybersecurity d.d. 29 juni 2023. TZ202307–065.

Vraag 10
Bent u voornemens het onderzoek van Interpolis, waarnaar verwezen wordt in het artikel, mee te nemen in de aanpak tegen phishing en andere vormen van cybercriminaliteit? Zo ja, op welke manier zal dit terugkomen en wanneer verwacht het kabinet een update over de aanpak te kunnen geven? Zo nee, waarom niet?

Antwoord 10
De in het artikel genoemde noties over online weerbaarheid, en het herkennen en voorkomen van cybercriminaliteit zijn bekend. Dat wordt door de Minister van Justitie en Veiligheid meegenomen in de aanpak tegen cybercrime, en de aanpak tegen online fraude. Een voorbeeld hiervan is de campagne «Laat je niet interneppen», die op 10 oktober is gestart. Er wordt rekening gehouden met de verschillende (online) belevingswerelden van verschillende leeftijdsgroepen. Daarom is het eerste deel van de campagne met name gericht op jongeren tussen 15 en 23 jaar oud. Volgende delen zullen zich op andere doelgroepen richten.
In het voorjaar van 2024 zal de Minister van Justitie en Veiligheid een volgende update over de integrale aanpak cybercrime naar uw Kamer zenden.

Vraag 11
De drempel om te starten met cybercrime zoals phishing ligt steeds lager en daders worden steeds jonger. De Minister heeft eerder toegezegd programma's als «Hack_Right» meer in te zetten om jongeren op het juiste pad te zetten: hoe staat het hiermee? Hoe vaak is een hack_right traject in 2023 tot dus ver opgelegd?

Antwoord 11
Er zijn verschillende interventies die door de politie en HALT worden ingezet om jongeren op het juiste te pad te houden of te zetten. Een voorbeeld hiervan is Re_B00tcmp, een terugkerend regionaal evenement voor jongeren met interesse in IT, en die de neiging hebben online grenzen op te zoeken. Tijdens het evenement leren zij middels verschillende presentaties van publieke en private partijen over online grenzen en positieve kansen van IT. Ook is er lesmateriaal ontwikkeld, dat ondersteuning biedt aan ouders, docenten en wijkagenten om jongeren met interesse in IT naar diverse positieve alternatieven te begeleiden. Ook is een aantal online interventies ontwikkeld, zoals de game Framed, en de inkoop van online advertenties om mensen die naar cybercriminele activiteiten (zoals DDoS) zoeken een advertentie van de politie te laten zien die informeert over de strafbaarheid en mogelijke consequenties. In 2023 zijn er tot dusver twee Hack_Right-trajecten opgelegd. Daarnaast is Hack_Right twee keer geadviseerd, eenmaal door de Raad van de Kinderbescherming, en eenmaal door de Reclassering. De rechter heeft daarover nog geen uitspraak gedaan.