Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

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

913

Vragen van de leden **Oosenbrug** en **Kerstens** (beiden PvdA) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Sociale Zaken en Werkgelegenheid over *lekke overheidswebsites* (ingezonden 2 december 2016).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister van Sociale Zaken en Werkgelegenheid (ontvangen 10 januari 2016).

Vraag 1
Kent u de berichten «Helft websites overheid onveilig»[1] en «Veel overheid websites onnodig onveilig»[2]?

Antwoord 1
Ja.

Vraag 2
Is het waar dat van de 1.816 onderzochte websites van de Nederlandse overheid er minder dan de helft een verbinding heeft die ervoor zorgt dat het websiteverkeer versleuteld wordt? Zo nee, hoeveel zijn het er dan wel?

Antwoord 2
Het in de media geschetste beeld dat de verbindingen naar veel overheidswebsites niet goed beveiligd zijn, verdient enige nuance. Het belang van het beveiligen van de verbinding naar een overheidswebsite hangt af van of de website (persoons-) gevoelige informatie uitwisselt. Daarom zijn organisaties zelf verantwoordelijk voor het beveiligen van hun websites.
Het kabinet onderschrijft het belang van versleuteling. Om de implementatie van versleutelde verbindingen te versnellen, heeft het Nationaal Beraad Digitale Overheid in februari van dit jaar overheidsbreed het streefbeeld afgesproken om uiterlijk eind 2017 versleutelde verbindingen overal op overheidswebsites te hebben toegepast, waar persoonsgegevens of andere gevoelige gegevens aan de orde zijn. Deze afspraak is op advies van het Forum Standaardisatie tot stand gekomen en ligt in het verlengde van de

[1] http://m.binnenlandsbestuur.nl/nieuws/helft-websites-overheid-onveilig.124902.lynkx
[2] https://openstate.eu/nl/2016/12/open-state-lanceert-pulse-veel-overheid-websites-onnodig-onveilig/

ah-tk-20162017-913
ISSN 0921 - 7398
's-Gravenhage 2017

eerdere opname van de achterliggende TLS-standaard op de «pas toe of leg uit»-lijst die geldt bij nieuwe investeringen. Vanuit dat oogpunt zijn er in het nieuwe DigiD normenkader v2.0, dat geldt vanaf 1 juli 2017 en dat gebaseerd is op de vernieuwde versie van NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties (versie 2015), wijzigingen doorgevoerd.[3] Zo dienen veelgebruikte entreepagina's naar bijvoorbeeld contactformulieren ook met HTTPS beveiligd te zijn.

Vraag 3
Is het waar dat van de overheidswebsites die wel een https-verbinding gebruiken er ook nog een aantal websites is dat zodanig is ingesteld dat er ook daar een beveiligingsrisico bestaat? Zo nee, wat is er dan niet waar?

Antwoord 3
Inderdaad is het zo dat nog niet alle overheidswebsites zo zijn ingesteld dat er geen beveiligingsrisico bestaat. Elke overheidsorganisatie is uiteindelijk zelf verantwoordelijk voor het beveiligen van de eigen overheidswebsites.
De voortgang van de adoptie van beveiligingsstandaarden in websites en e-mail van de overheid wordt halfjaarlijks op verzoek van het Nationaal Beraad door het Forum Standaardisatie bij een set overheidsdomeinnamen gemeten. Zo wordt gekeken of de overheid op koers is ten aanzien van het streefbeeld dat is afgesproken in het Nationaal Beraad. In die meting wordt ook gekeken of de HTTPS-verbinding is geconfigureerd volgens het advies van het NCSC («ICT-beveiligingsrichtijnen voor TLS»). Dat is namelijk inderdaad óók van belang. Zowel op het gebied van de toepassing van HTTPS als de veilige configuratie conform NCSC-advies, wordt flinke vooruitgang geboekt.[4]
De metingen worden uitgevoerd met behulp van de testtool https://internet.nl. Deze testtool staat ook ter beschikking aan alle overheden. De tool is ontwikkeld door het Platform Internetstandaarden, dat een samenwerkingsverband is van de Nederlandse internetcommunity en overheid.
Om de adoptie van HTTPS te versnellen worden, naast de streefbeeldafspraak, metingen en de testtool, aanvullende acties ondernomen. De Informatie Beveiligings Dienst (IBD) van VNG/KING adviseert gemeenten om HTTPS te gebruiken en te configureren conform NCSC-advies. Ter ondersteuning hebben zij in samenwerking met Forum Standaardisatie een factsheet ontwikkeld voor het toepassen van HTTPS op gemeentelijk niveau en zijn er diverse workshops georganiseerd in het land.

Vraag 4
Is de conclusie uit het onderzoek van Open State dat er een beveiligingsrisico is bij 62 procent van de overheidswebsites gerechtvaardigd? Zo ja, deelt u dan de mening dat dit een schrikbarende conclusie is en waarom? Zo nee, waarom is die conclusie niet gerechtvaardigd?

Antwoord 4
Het is onwenselijk wanneer websiteonderdelen waar gevoelige gegevens zoals financiële en/of persoonsgegevens, worden verwerkt, onversleuteld zijn. Vandaar dat is ingezet op het afgesproken streefbeeld om HTTPS op die plekken overal toe te passen.

Vraag 5
Behoort het UWV (Uitvoeringsorgaan werknemersverzekeringen) tot de groep met een site die onveilig is? Zo ja, hoe kan dat en hoe wordt dat snel opgelost? Zo ja, wat kunnen de gevolgen zijn voor de bescherming van gevoelige persoonsgegevens of andere gegevens?

---

[3] https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/

[4] Zie de «Meting informatiebeveiligingsstandaarden» Monitor Open Standaarden #2, https://magazine.forumstandaardisatie.nl

Antwoord 5
Websites van UWV (uwv.nl en bkwi.nl) worden genoemd op de lijst van het OSF, omdat zij geen gebruik maken van een https-verbinding. Het gedeelte van uwv.nl waarop algemene informatie wordt getoond (de landingspagina) gebruikt een http-verbinding. Voor deze pagina staat een softwarematige omzetting naar HTTPS in het tweede kwartaal van 2017 op de planning. Pagina's van uwv.nl waar sprake is van gegevensuitwisseling (bijv. tonen van persoonsgegevens door UWV, insturen van gegevens door klanten) bevinden zich in de MijnUWV-omgeving. Deze pagina's zijn wel voorzien van een HTTPS-verbinding. Om in de MijnUWV-omgeving te komen moet bovendien worden ingelogd met DigiD. Op de website bkwi.nl wordt enkel informatie getoond die betrekking heeft op de gegevensleveringen die BKWI faciliteert. Er wordt geen informatie getoond die betrekking heeft op personen. Vooruitlopend op de vernieuwing van bkwi.nl in het eerste kwartaal van 2017 wordt de site eind 2016 voorzien van een HTTPS-verbinding. Werk.nl maakt wel gebruik van een HTTPS-verbinding. In de huidige situatie worden gevoelige persoonsgegevens adequaat beschermd.

Vraag 6
Welke risico's brengen slecht beveiligde overheidswebsites met zich mee?

Antwoord 6
Wanneer websites geen gebruik maken van versleuteling bij de communicatie, is het mogelijk dat derden de informatie in kunnen zien die opgevraagd wordt, deze eventueel kunnen veranderen of voorzien van bijvoorbeeld malware. In het geval dat er een transactie plaatsvindt, kan deze mogelijk ook gemanipuleerd worden. Het toepassen van HTTPS en van een bijbehorend certificaat helpt om de authenticiteit van een overheidswebsite te kunnen controleren en kan daardoor phishing voorkomen. Voor iedere website en dienst zal een aparte risicoafweging gemaakt moeten worden door de verantwoordelijke overheidsorganisaties. Daarbij is van belang te vermelden dat alle privacygevoelige overheidswebsites eind 2017 beveiligd moeten worden volgens de HTTPS richtlijnen zoals afgesproken in het Nationaal Beraad.

Vraag 7
Deelt u de mening van o.a. Bits of Freedom dat het onbegrijpelijk is dat de overheid dit niet beter doet? Zo ja, welke conclusies en welk gevolg verbindt u hieraan? Zo nee, waarom deelt u die mening niet?

Antwoord 7
Ik deel die mening niet. Zie mijn antwoord op vraag 2, 3 en 4.