Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
http://www.rijksoverheid.nl

Kenmerk
2016-0000807510

Uw kenmerk
2016Z22934

Datum 9 januari 2017

Betreft Beantwoording Kamervragen over het bericht 'Veel' overheidssites hebben geen beveiligde verbinding'

Hierbij bied ik u de antwoorden aan op de schriftelijke vragen die zijn gesteld door het lid Amhaouch (CDA) over het bericht 'Veel overheidssites hebben geen beveiligde verbinding'.

Deze vragen werden ingezonden op 2 december 2016, met kenmerk 2016Z22934.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Datum

Kenmerk
2016-0000807510

2016Z22934

Vragen van het lid Amhaouch (CDA) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over het artikel 'Veel overheidssites hebben geen beveiligde verbinding' (ingezonden 2 december 2016)

Vraag 1
Kent u het artikel 'Veel overheidssites hebben geen beveiligde verbinding'? 1)

Antwoord 1
Ja.

Vraag 2
Is het waar, dat de verbindingen naar veel overheidswebsites niet goed beveiligd zijn?

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 staat daarbij buiten kijf dat bij het beveiligen van verbindingen naar overheidswebsites het volgen van bepaalde gestelde standaarden en best practices, bijvoorbeeld de richtlijnen van het NCSC, gewenst is. Volgens de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties moeten overheidswebsites waarbij gevoelige gegevens worden ingevoerd, zoals bij een contactformulier of wanneer gegevens vooringevuld zijn, onder andere voldoen aan de TLS-standaard (Transport Layer Security, de standaard onder HTTPS). De implementatie van de TLS standaard dient vervolgens te voldoen aan de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security.

TLS is ook opgenomen op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie en aanvullend is over TLS op advies van Forum Standaardisatie door het Nationaal Beraad Digitale Overheid een adoptie-impuls (‘streefbeeld’) afgesproken.

Het Forum Standaardisatie voert op verzoek van het Nationaal Beraad Digitale Overheid, met behulp van de testtool https://internet.nl, halfjaarlijkse metingen uit om de voortgang van de implementatie van de adoptieafspraak over TLS te monitoren. Daarbij moet worden vermeld dat de domeinnamen die worden gebruikt voor deze metingen slechts ten dele overeenkomen met de domeinnamen die OSF heeft gebruikt.

In de meting voor het Nationaal Beraad worden totaal 152 domeinnamen van Rijk, uitvoeringsorganisaties, provincies en waterschappen gemeten. Daarover wordt in de laatste meting gerapporteerd: “TLS was en is met afstand de meest toegepaste standaard (75% van de gemeten domeinnamen bij

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Datum

Kenmerk
2016-0000807510

uitvoeringsorganisaties, provincies en waterschappen) [in vergelijking met de andere gemeten informatiebeveiligingsstandaarden]. Hierdoor is de relatieve groei van TLS beperkt. Daarentegen is het aantal sites dat conform de ICT-beveiligingsrichtlijnen voor TLS op de door het NCSC voorgeschreven veilige manier (volgens het veel strengere normenkader van DigiD veiligheidsrichtlijnen) is geconfigureerd over het afgelopen jaar flink gestegen (23% naar 40%) ."[1]

Daarnaast zijn 398 gemeentelijke domeinnamen gemeten; daarover wordt opgemerkt: "Wat vooral opvalt is dat de initiële adoptiegraad van TLS midden 2015 al erg hoog lag (80%) en is gegroeid naar 82% in 2016. Daarbij kan wel worden opgemerkt dat, vergeleken met de niet-gemeentelijke domeinen, het aantal domeinen waarbij TLS is geconfigureerd volgens de aanbevelingen van het NCSC relatief laag is (21%)". Domeinen waar persoonsgegevens uit worden gewisseld zijn beveiligd via de HTTPS/TLS standaard. Vanuit het Nationaal Beraad van begin 2016 is ook een adoptieafspraak gemaakt voor alle overheidsdomeinen, landingspagina's en voor domeinen zonder uitwisseling van persoonsgegevens. Eind 2017 moeten ook deze pagina's voldoen aan de adoptieafspraak voor HTTPS/TLS standaarden.

Vraag 3
Deelt u de mening dat een goede beveiliging van overheidswebsites noodzakelijk is voor het handelen tussen burger en overheid?

Antwoord 3
Ja.

Vraag 4
Welke maatregelen zijn er reeds genomen om een veilige verbinding met overheidswebsites tot stand te brengen?

Antwoord 4
Beveiligde (oftewel versleutelde) verbindingen met websites werken op basis van HTTPS en de onderliggende TLS-standaard. Het kabinet onderschrijft het belang van versleuteling. Om de implementatie van versleutelde verbindingen te versnellen heeft het Nationaal Beraad 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 persoons- of financiële gegevens aan de orde zijn. Voor geheel informatieve websites geldt deze afspraak niet. Bij de implementatie van TLS worden de 'ICT-beveiligingsrichtlijnen voor TLS' (versie 2012) van het NCSC gevolgd. Deze afspraak is op advies van het Forum Standaardisatie tot stand gekomen en ligt in het verlengde van de eerdere opname van de achterliggende TLS-standaard op de 'pas toe of leg uit'-lijst die geldt bij nieuwe investeringen. Met de eerder genoemde metingen houdt het Nationaal Beraad de voortgang bij.

[1] Zie de "Meting informatiebeveiligingssstandaarden" Monitor Open Standaarden #2, https://magazine.forumstandaardisatie.nl

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Datum

Kenmerk
2016-0000807510

Daarnaast worden overheidswebsites die gebruik maken van DigiD getoetst aan de 'Norm ICT-beveiligingsassessments DigiD', die is gebaseerd op de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het NCSC. In het kader van DigiD zijn de richtlijnen die de meeste impact hebben op de veiligheid van DigiD en de met DigiD ontsloten gegevens gekwalificeerd als de DigiD-norm en onderdeel van de beveiligingsassessments. De DigiD-norm verplicht onder andere de toepassing van HTTPS. Organisaties toetsen in dit kader eerst zelf in hoeverre de systemen voldoen. Daarna volgen een penetratietest ofwel Ethical Hack en een audit. Vanaf 1 juli 2017 geldt het nieuwe normenkader v2.0, gebaseerd op de vernieuwde versie van NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties (versie 2015).[2] Veelgebruikte entreepagina's naar bijvoorbeeld contactformulieren dienen dan ook met HTTPS beveiligd te zijn.

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. Daarnaast worden standaarden ingevoerd bij nieuwe ICT investeringen (de zogeheten pas-toe-of-leg-uit lijst van het Forum Standaardisatie). Via de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) worden leveranciers verplicht deze standaarden te leveren.

Vraag 5
Bent u van mening dat de geloofwaardigheid van de overheid wordt aangetast doordat de beveiliging van veel overheidswebsites niet voldoende is terwijl internetbeveiliging juist een hoge prioriteit heeft in het overheidsbeleid?

Antwoord 5
Vooropgesteld is het beveiligen van overheidswebsites natuurlijk van belang, maar op basis van het aangehaalde onderzoek kan ik niet concluderen dat de overheidswebsites in het algemeen niet voldoen. De maatregelen zoals deze zijn opgetekend in het antwoord op vraag 4 dragen bij aan het beveiligen van de overheidswebsites.

Vraag 6
Welke maatregelen neemt u om ervoor te zorgen dat de veiligheid van overheidswebsites zo spoedig mogelijk substantieel verbeterd wordt?

Antwoord 6
In de beantwoording van vraag vier zijn verschillende maatregelen naar voren gekomen. Op grond van de Wet bescherming persoonsgegevens is de verwerker verantwoordelijk voor de verwerking van persoonsgegevens, dus de eigenaar van de website, zelf verplicht zorg te dragen voor passende technische en organisatorische maatregelen. Het versleutelen van het verkeer via een https-

2
https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Datum

Kenmerk
2016-0000807510

verbinding is een voorbeeld van een dergelijke maatregel. De Autoriteit Persoonsgegevens (AP) ziet hierop toe.

1) http://nos.nl/artikel/2145883-veel-overheidssites-hebben-geen-beveiligde-verbinding.html

Toelichting:
Deze vragen dienen ter aanvulling op eerdere vragen terzake van de leden Oosenbrug en Kerstens (beiden PvdA), ingezonden 2 december 2016 (vraagnummer 2016Z22925)