Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Binnenhof 4
Den Haag

Directie Bedrijfsvoering
Bezuidenhoutseweg 67
2594 AC Den Haag
Postbus 20061
Nederland
www.rijksoverheid.nl

Onze Referentie
BZDOC-1121086010-84
Uw Referentie
2017Z03930
Bijlage(n)

Datum 30 mei 2017
Betreft Beantwoording vragen van het lid Ten Broeke over de beveiliging van websites van Nederlandse ambassades.

Hierbij bieden wij de antwoorden aan op de schriftelijke vragen gesteld door het lid Ten Broeke over de beveiliging van websites van Nederlandse ambassades. Deze vragen werden ingezonden op 22 maart 2017 met kenmerk 2017Z03930

De Minister van Buitenlandse Zaken,

Bert Koenders

Antwoorden van de Minister van Buitenlandse Zaken op vragen van het lid Ten Broeke (VVD) over de beveiliging van websites van Nederlandse ambassades,

Directie Bedrijfsvoering

Onze Referentie
BZDOC-1121086010-84

Vraag 1
Hoe beoordeelt u de berichtgeving over de inadequate beveiliging van websites van Nederlandse ambassades?[1] Klopt het dat de websites van de Nederlandse ambassades in Afghanistan, China, Egypte en Soedan nog altijd onvoldoende zijn beveiligd?

Vraag 3
Klopt het dat deze risico's al enige tijd bekend zijn bij uw ministerie en dat bezoekers al maanden onnodig veel risico lopen?

Vraag 4
Wanneer verwacht u een oplossing te hebben voor het beveiligingsprobleem?

Antwoord vraag 1, 3 en 4
Nee, het klopt niet dat de websites van de Nederlandse ambassades in de vier genoemde landen nog altijd onvoldoende zijn beveiligd.

Op 4 april jongstleden zijn de nieuwe websites van het ministerie www.nederlandwereldwijd.nl en www.nederlandenu.nl gelanceerd, die onder andere de genoemde websites van de posten vervangen. Deze nieuwe sites gebruiken voor de beveiliging onder andere het HTTPS communicatieprotocol en dwingen het gebruik daarvan door de browsers van bezoekers af.

De berichtgeving betrof de constatering dat een groot percentage overheidswebsites voor hun beveiliging het HTTPS communicatieprotocol niet of niet goed ingericht hadden voor hun websites. Zie hiervoor tevens de beantwoording van de kamervragen van Amhaouch[2] en Oosenburg/Kerstens[3] eerder dit jaar.

De in de vragen genoemde websites maakten ten tijde van de berichtgeving niet voor alle pagina's van de websites gebruik van het HTTPS communicatieprotocol en dwongen het gebruik daarvan ook niet af voor de browser van bezoekers. De noodzakelijk geachte mate van het beveiligen van de verbinding naar een overheidswebsite hangt af van de vraag of de website (persoons-) al dan niet

---

[1] Binnenlands Bestuur, 10 maart 2017, 'Beveiliging overheidssites nog steeds niet op orde', http://www.binnenlandsbestuur.nl/digitaal/nieuws/beveiliging-overheidssites-nog-steeds-niet-op.9559719.lynkx

[2] Kamervraag 912: https://www.tweedekamer.nl/downloads/document?id=33640960-6d0b-4c37-a59c-0259bde16d8f&title=Antwoord%20op%20vragen%20van%20het%20lid%20Amhaouch%20over%20het%20artikel%20%27Veel%20overheidssites%20hebben%20geen%20beveiligde%20verbinding%27.pdf

[3] Kamervraag 913: https://www.tweedekamer.nl/downloads/document?id=a29ae642-612d-4cb6-9587-b2844fce4c2a&title=Antwoord%20op%20vragen%20van%20de%20leden%20Oosenbrug%20en%20Kerstens%20over%20de%20berichten%20%E2%80%98Helft%20websites%20overheid%20onveilig%E2%80%99%20en%20%E2%80%98Veel%20overheid%20websites%20onnodig%20onveilig%E2%80%99.pdf

gevoelige informatie uitwisselt. In de genoemde websites werd niet naar persoonsgevoelige informatie gevraagd, zodat het veiligheidsrisico gering was.

Het ministerie heeft recentelijk een omvangrijk project afgerond om de ruim 240 websites van de posten, waartoe de genoemde websites behoorden, te vervangen door twee nieuwe websites: www.nederlandwereldwijd.nl en www.nederlandenu.nl. De beveiliging van de nieuwe websites is ingericht conform de meest recente beveiligingseisen, inclusief het afdwingen van het HTTPS communicatieprotocol voor de gehele websites. Hiermee voldoen deze websites - ruim voor de deadline (eind 2017)die het Nationaal Beraad Digitale Overheid daarvoor vaststelde - aan de eis van het gebruiken van versleutelde verbindingen op overheidswebsites.

Vraag 2
Wat zijn de risico's voor bezoekers van deze websites, aangezien er geen veilige verbinding via HTTPS tot stand kan worden gebracht omdat bezoekers worden terug verwezen naar een HTTP-website?

Antwoord
HTTPS is een communicatieprotocol dat ervoor zorgt dat bezoekers de identiteit van de webserver / website kunnen controleren. Voorts beveiligt HTTPS de communicatie tussen de webserver en de browser door deze te versleutelen. Het protocol beveiligt in belangrijke mate tegen het afluisteren en het manipuleren van de communicatie tussen de webserver en de browser.
Het risico voor de bezoekers van een website zonder HTTPS is beperkt indien er geen (persoons-)vertrouwelijke informatie wordt uitgewisseld, zoals bij de betreffende websites het geval was.