FS-20230208-2F

FAQ over verplichting HTTPS en HSTS voor overheidswebsites

Doel: publicatie op website digitaleoverheid.nl

Doelgroep: bestuurder, ICT-manager, geïnteresseerde burger

Datum: 24 april 2022

Opsteller: Bart Knubben (Bureau Forum Standaardisatie)

Betreft eindconcept, wordt nog door BZK gepubliceerd op www.digitaleoverheid.nl

---

1. Wat wordt verplicht?

Het voorgenomen "Besluit beveiligde verbinding met overheidswebsites en -webapplicaties" verplicht overheidsorganisaties om hun publiek toegankelijke websites te beveiligen met de open standaarden HTTPS en HSTS. Daarbij moet de configuratie van beide standaarden voldoen aan de in het besluit genoemde richtlijnen van NCSC.

2. Waarom worden HTTPS en HSTS voor overheidswebsites verplicht? (Wat hebben burgers en ondernemers eraan?)

Gebruikers van overheidswebsites moeten erop kunnen vertrouwen dat informatie-uitwisseling vertrouwelijk verloopt. HTTPS en HSTS helpen daarbij. Deze beveiligingsstandaarden zorgen ervoor zorgen dat de verbinding met de website is versleuteld en dat de website daadwerkelijk hoort bij de gebruikte domeinnaam. Dit maakt het veel moeilijker voor kwaadwillenden om de informatie-uitwisseling tussen de burger/ondernemer en de overheidswebsite te onderscheppen oftewel 'af te luisteren'.

3. Voor welke overheidswebsites geldt de verplichting?

De verplichting geldt voor zowel interactieve websites, al dan niet na inloggen, waarmee informatie wordt uitgewisseld met een bezoeker (bijvoorbeeld doormiddel van een applicatie of formulieren) als voor websites waar (statische) informatie wordt weergegeven. Webapplicaties en web application programming interfaces (web API's) vallen dus ook onder deze verplichting.

Intranet sites die niet publiekelijk bereikbaar zijn vanaf internet, vallen buiten het toepassingsbereik van de verplichting. Dat wil overigens niet zeggen dat toepassing van de standaarden daar niet verstandig is.

4. Voor wie geldt de verplichting?

De verplichting tot toepassing van de standaarden geldt voor overheidsorganisaties die bestuursorgaan zijn als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht. Bij deze zogeheten a-bestuursorganen gaat het om de organen van de Staat (mits niet uitgezonderd), provincies, gemeenten, waterschappen en andere rechtspersonen die krachtens publiekrecht zijn ingesteld.

5. Wat is de grondslag voor de verplichting?

De verplichting is vastgelegd in het "Besluit beveiligde verbinding met overheidswebsites en -webapplicaties". De grondslag voor dit besluit is artikel 3, tweede lid, van de

aangekondigde Wet digitale overheid op basis waarvan standaarden voor elektronisch verkeer kunnen worden aangewezen, die overheidsorganisaties verplicht moeten toepassen. De Wet digitale overheid is op dit moment in behandeling door de Eerste Kamer.

6. Wanneer gaat de verplichting in?

De verplichting van HTTPS en HSTS voor overheidswebsites zal naar verwachting ingaan kort nadat de Wet digitale overheid in werking is getreden. Naar verwachting is dat (op het moment van schrijven van deze FAQ) op zijn vroegst op 1 juli 2022.

7. Hoe kan je zien of een overheidswebsite voldoet aan de verplichting?

Een gebruiker ziet in zijn/haar webbrowser een slotje in de URL-balk naast de domeinnaam van de website, indien een website HTTPS ondersteunt. Het slotje zegt alleen nog niets over het gebruik van HSTS en de relevante NCSC-richtlijnen. Met de testtool Internet.nl van eenieder testen of een overheidswebsite volledig voldoet aan de verplichting. Een website die voldoet moet slagen voor alle subtesten in de categorie "Beveiligde verbinding (HTTPS)" van de websitetest. De categorie omvat ook testen voor HSTS en de richtlijnen van NCSC.

8. Hoe past deze verplichting bij reeds ingezet beleid?

Het verplicht voorschrijven van deze standaarden is een vervolg op ingezet beleid.

Sinds 2014 bestaat voor overheden een 'aanschafverplichting' voor de achterliggende TLS-standaard toen deze op advies van het Forum Standaardisatie werd geplaatst op de 'pas toe of leg uit'-lijst met open standaarden. In 2017 volgden de HTTPS- en HSTS-standaard. Met de opname ontstond de verplichting voor overheidsorganisaties om bij de aanschaf van websites en webapplicaties deze standaarden te vereisen. Afwijken is alleen toegestaan bij zwaarwegende redenen en bovendien moet een overheidsorganisatie daarover uitleg geven in het jaarverslag.

Begin 2016 ontstond een eerste 'gebruiksverplichting' toen het Nationaal Beraad Digitale Overheid op advies van Forum Standaardisatie de overheidsbrede streefbeeldafspraak maakte om TLS (in de vorm van HTTPS) toe te passen bij alle overheidswebsites waarbij burgers en of bedrijven gegevens moet invoeren, of waarbij gegevens vooringevuld zijn. In februari 2017 zegde de minister van Binnenlandse Zaken en Koninkrijksrelaties de Tweede Kamer toe om de toepassing van de HTTPS-standaard bij overheidswebsites te verplichten.

Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) breidde begin 2018 de bestaande streefbeeldafspraak uit en bepaalde dat alle overheidswebsites HTTPS en HSTS moesten ondersteunen voor het einde van 2018 en dat deze conform de richtlijnen van het Nationaal Cyber Security Centrum (hierna: NCSC) moesten zijn geconfigureerd.

9. Wat is het huidige gebruik onder overheidsorganisaties?

Forum Standaardisatie voert sinds 2016 periodieke metingen uit naar het gebruik van HTTPS en HSTS onder overheidsorganisaties inclusief de relevante NCSC-richtlijnen.

Uit de meting van maart 2019, korte tijd na afloop van de OBDO-streefbeeldafspraak, bleek dat het streefbeeld voor HTTPS en HSTS niet is gehaald. Bij 89% van de ongeveer 560 getoetste kern-overheidswebsites werd HTTPS gebruikt en geconfigureerd volgens de richtlijnen van het NCSC. 79% van de getoetste sites gebruikte HSTS.

In latere metingen is ook een grotere set van circa 2200 overheidsdomeinnamen gemeten. Daaruit blijkt dat de toepassingsgraad van HTTPS en HSTS buiten de kern-

overheidswebsites lager ligt. Uit de laatste meting van september 2021 komt naar voren dat bij 70% van de websites van de uitgebreide set 'HTTPS conform NCSC-richtlijnen' is geconfigureerd en dat bij 63% HSTS wordt ondersteunt.

10. Hoe is de verplichting tot stand gekomen?

Door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is in samenwerking met Forum Standaardisatie het ontwerpbesluit "beveiligde verbinding met overheidswebsites en -webapplicaties" opgesteld en zijn daarbij de vragen van het "Integraal Afwegingskader voor beleid en regelgeving" (IAK) beantwoord.

Het ontwerpbesluit is publiekelijk geconsulteerd van 2 september 2019 tot en met 20 oktober 2019. In totaal zijn 13 reacties binnengekomen. De noodzaak van het verplicht stellen van de standaarden HTTPS en HSTS werd door nagenoeg alle respondenten onderschreven. Over de ontvangen consultatie heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een verslag gepubliceerd.

11. Zegt de verplichting ook wat over het type TLS-certificaat dat moet worden gebruikt?

Het toepassen van HTTPS betekent dat partijen een TLS-certificaat moeten installeren op hun website. Het voorgenomen besluit schrijft geen specifiek type TLS-certificaat, zoals bijvoorbeeld van PKIoverheid, voor. Voor meer informatie over certificaten en de keuze van een certificaatleverancier kan worden verwezen naar factsheet "PKIoverheid stopt met webcertificaten" van NCSC.

12. Worden andere beveiligingsstandaarden ook verplicht?

Naast HTTPS en HSTS zijn voor websites ook andere beveiligingsstandaarden, zoals DNSSEC, van belang. Daarnaast zijn er belangrijke beveiligingsstandaarden voor andere toepassingen, zoals DMARC en DANE voor e-mail. In de consultatie stelden ook verschillende respondenten voor om ook andere open standaarden te verplichten. Voor verschillende van deze standaarden bestaan reeds minder vergaande verplichtingen in de vorm van 'pas toe of leg uit' en 'streefbeeldafspraken'. Nadat het voorgenomen besluit voor verplichte toepassing van de informatieveiligheidsstandaarden HTTPS en HSTS in werking is getreden, zal de regering zich beraden voor welke standaard(en) het opportuun is om ook een besluit tot verplichte toepassing te nemen.

13. Hoe zijn het toezicht en de handhaving geregeld?

Uit ontwerpbesluit:

"Het toezicht op de naleving vindt plaats overeenkomstig het bepaalde in hoofdstuk 6 van de Wdo. De minister op wiens beleidsterrein het betreffende bestuursorgaan werkzaam is, houdt toezicht op bestuursorganen op het niveau van het Rijk. Voor het overige geldt het reguliere interbestuurlijk toezicht.

Het Forum Standaardisatie meet jaarlijks in hoeverre de standaarden op de 'pas toe of leg uit'-lijst worden toegepast. Door de minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen open standaarden worden hierin meegenomen. De uitkomsten van de meting worden besproken in het Forum Standaardisatie en het OBDO en vervolgens aan de Tweede Kamer overgelegd. Op deze wijze wordt transparant welke specifieke organen al dan niet voldoen aan de verplichting.

Het belang dat burgers, bedrijven en bestuursorganen zelf hebben bij de toepassing van de standaarden, alsook de bestaande monitoring en het beoogde toezichtsmechanisme,

acht de regering afdoende om te borgen dat de verplichting wordt nageleefd door bestuursorganen."

Uit voorstel Wdo:

"Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld. Onder meer kan worden bepaald dat organen op hun website een actuele verklaring over de toepassing van de aangewezen standaard publiceren en kan worden bepaald dat organen aan Onze Minister een verklaring van een auditor overleggen waaruit blijkt of de aangewezen standaard wordt toegepast. In voorkomend geval worden regels gesteld over de wijze van rapportage respectievelijk publicatie."

"Onze Minister kan een aanwijzing geven aan een orgaan waarvoor de verplichting tot toepassing van een aangewezen standaard geldt, indien dit orgaan een gedragslijn hanteert die strijdig is met een aangewezen standaard."