Besluit van
houdende aanwijzing van de open informatieveiligheidsstandaarden HTTPS en HSTS voor websites en webapplicaties van bestuursorganen (Besluit beveiligde verbinding met overheidswebsites en -webapplicaties)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van [datum], nr. [nummer];

Gelet op artikel 3, tweede en vierde lid, van de Wet digitale overheid;

De Afdeling advisering van de Raad van State gehoord (advies van [datum], nr. [nummer]);

Gezien het nader rapport van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van [datum], nr. [nummer];

Hebben goedgevonden en verstaan:

Artikel 1. Definities

In dit besluit wordt verstaan onder:

a. *HSTS*: de 'HTTP Strict Transport Security', IETF RFC 6797;
b. *HTTPS*: de 'HyperText Transfer Protocol Secure', IETF RFC 2818;
c. *TLS-richtlijn*: de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.0, gepubliceerd op https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls;
d. *Webapplicatie-richtlijn*: de ICT-Beveiligingsrichtlijnen voor Webapplicaties, versie 2015, gepubliceerd op https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.

Artikel 2. Aanwijzing

Bestuursorganen als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht, beveiligen hun publiek toegankelijke websites en webapplicaties door toepassing van HTTPS en HSTS, met dien verstande dat:

a. de standaarden worden geconfigureerd overeenkomstig de instellingen die de status voldoende of goed krijgen in de TLS-richtlijn; en
b. maatregel 5 bij beveiligingsrichtlijn U/WA.05 van de Webapplicatie-richtlijn wordt toegepast.

Artikel 3. Inwerkingtreding

Dit besluit treedt in werking met ingang van [datum].

Artikel 4. Citeertitel

Dit besluit wordt aangehaald als: Besluit beveiligde verbinding met overheidswebsites en -webapplicaties.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

NOTA VAN TOELICHTING

Algemeen deel

1. Inleiding

Met dit besluit wordt de toepassing van de informatieveiligheidsstandaarden HTTPS en HSTS verplicht voorgeschreven voor publiek toegankelijke websites[1] van bestuursorganen. Het besluit heeft tot doel de beveiliging van deze websites te bevorderen. Gebruikers van overheidswebsites moeten erop kunnen vertrouwen dat informatie-uitwisseling vertrouwelijk verloopt doordat de verbinding met website beveiligd is, dat de informatie van de website daadwerkelijk afkomstig is van de beheerder van de website en dat de website daadwerkelijk hoort bij de gebruikte domeinnaam.

2. Aanleiding

In februari 2017 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties de Tweede Kamer toegezegd om de toepassing van de HTTPS-standaard bij overheidswebsites te verplichten.[2] Het verplicht voorschrijven van deze standaarden is een vervolg op ingezet beleid. Voor de HTTPS- en HSTS-standaard geldt momenteel het zogenaamde ‘pas toe of leg uit’-beleid voor open standaarden. Dit beleid houdt kort gezegd in dat op het moment dat een bestuursorgaan investeert in een ICT-systeem of -dienst, de relevante standaarden van de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie dienen te worden toegepast (pas toe). Bestuursorganen hebben de mogelijkheid af te wijken van de opgenomen standaarden indien hiervoor een zwaarwegende reden is (leg uit).

Het Nationaal Beraad Digitale Overheid sprak begin 2016 de ambitie uit om een aantal informatieveiligheidsstandaarden, waaronder de HTTPS-standaard, overal waar relevant, te implementeren. Het Nationaal Beraad was van mening dat de urgentie voor deze standaarden dermate hoog is dat deze direct dienen te worden toegepast. Voor deze standaarden zijn er geen zwaarwegende redenen te noemen om deze niet toe te passen. Bovendien geldt dat een gebrekkige informatiebeveiliging van één overheidspartij negatief afstraalt op de gehele overheid. Hierom werd vrijblijvendheid om zelf een toepassingsmoment te kiezen niet wenselijk geacht.[3]

Begin 2018 is het Nationaal Beraad opgevolgd door het Overheidsbreed Beleidsoverleg Digitale Overheid (hierna: OBDO).[4] Het OBDO besloot begin 2018 het streefbeeld van het Nationaal Beraad uit te breiden, opdat *alle* overheidswebsites HTTPS en HSTS

[1] Omwille van de leesbaarheid wordt in deze Toelichting alleen het begrip ‘websites’ gebruikt. Dit dient gelezen te worden als ‘websites en webapplicaties’.
[2] *Kamerstukken II 2016/17,* 26643, nr. 443, p. 11-12 en *Kamerstukken II 2018/19,* 26643, nr. 574, p. 5-6.
[3] https://digitaleoverheid.pleio.nl/file/download/44041112.
[4] *Stcrt*. 2018, nr. 9728.

ondersteunen voor het einde van 2018 en deze conform de richtlijnen van het Nationaal Cyber Security Centrum (hierna: NCSC) zijn geconfigureerd.

Op verzoek van het OBDO toetst het Forum Standaardisatie iedere zes maanden circa 560 publiek toegankelijke overheidswebsites op de toepassing van de informatieveiligheidsstandaarden waarvoor het OBDO streefbeeldafspraken heeft gemaakt. Uit de meest recente meting van maart 2019 blijkt dat het streefbeeld voor HTTPS en HSTS niet is gehaald.[5] Bij 89% van de getoetste websites wordt HTTPS gebruikt en geconfigureerd volgens de richtlijnen van het NCSC. 79% van de getoetste sites gebruikt HSTS. Nu het huidige beleid niet tot gevolg heeft dat alle bestuursorganen de standaarden hebben geïmplementeerd, worden deze door middel van dit besluit dwingend voorgeschreven.

3. Noodzaak voor verplichtstelling

Met de groei van de afhankelijkheid van het internet zijn de risico's voor de veiligheid en privacy van bezoekers van websites eveneens toegenomen. Ieder internetgebruik dat bijvoorbeeld niet via HTTPS verloopt geeft informatie over het gedrag van de gebruiker en kan interessant zijn voor derden om te verzamelen. Het is daarom belangrijk dat bestuursorganen hun websites goed beveiligen.

Toepassing van de HTTPS-standaard borgt de vertrouwelijkheid, authenticiteit en integriteit van de berichtenuitwisseling. In combinatie met de HSTS-standaard wordt het moeilijker gemaakt om het berichtenverkeer dat via websites verloopt te onderscheppen.

De toepassing van HTTPS is inmiddels gemeengoed. Uit statistieken van Google blijkt dat van de honderd best bezochte websites ter wereld (samen goed voor 25% van het totale internetverkeer) 96% werkt met HTTPS.[6] Bij Googles eigen internetverkeer verloopt, afhankelijk van het land en gebruikte platform, tussen de 88% en 95% via HTTPS. Het wordt bovendien lastig om websites zonder HTTPS te vinden, omdat populaire zoekmachines websites zonder HTTPS lager in de zoekresultaten plaatsen. Daarnaast duiden verschillende browsers tegenwoordig websites zonder HTTPS aan als "onveilig".[7]

Ook andere overheden zetten in op de toepassing van HTTPS. Zo hanteert het CIO office van de federale overheid van de Verenigde Staten 'HTTPS for everything' als uitgangspunt. Zij stellen dat met de groei van de afhankelijkheid van het internet, de risico's voor de veiligheid en privacy van de gebruikers ook zijn gegroeid en de overheid daarom HTTPS moet toepassen op overheidswebsites, ongeacht het type website of type informatie dat wordt uitgewisseld.[8]

---

[5] https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken.
[6] https://transparencyreport.google.com/https/overview?load_os_region=chrome-usage:1;series:page-load;groupby:os&lu=load_os_region.
[7] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html en https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure#w_gray-padlock-with-red-strikethrough.
[8] https://https.app.cloud.gov/everything.

HTTPS-standaard

Het gebruik van HTTPS zorgt er allereerst voor dat de gegevens die de bezoeker en de website uitwisselen, worden versleuteld (vertrouwelijkheid). Hierdoor is het voor derden die gegevens onderscheppen, niet mogelijk om deze gegevens uit te lezen. Het gaat hier onder meer om de webcontent, URL's, cookies en andere gevoelige (meta)data.[9] Ook als er informatie wordt gedeeld via formulieren, wordt deze versleuteld verzonden, zodat een derde niet mee kan kijken.

Daarnaast stelt HTTPS de bezoeker in staat om te controleren of daadwerkelijk contact wordt gelegd met de website die hoort bij de gebruikte domeinnaam (authenticiteit). Door HTTPS kan worden voorkomen dat met een vervalste website (*spoofing*) of via een kwaadwillende tussenpersoon informatie wordt uitgewisseld.[10]

Tot slot waarborgt HTTPS dat een kwaadwillende de gegevens tussen de bezoeker en de website onderweg niet kan aanpassen of zaken (bijvoorbeeld *malware*) kan toevoegen (integriteit). Een bezoeker kan erop vertrouwen dat de informatie die wordt verschaft via de website of de doorverwijzing naar bijvoorbeeld een andere website, niet door anderen dan de beheerder van de website kan worden aangepast.

De toepassing van HTTPS is voor bezoekers websites te herkennen aan de weergave van het kenmerkende slotje in de adresbalk van de browser. Alleen als alle overheidswebsites HTTPS toepassen, kan een bezoeker van een overheidswebsite, het ontbreken van een ‘slotje’ interpreteren als een aanwijzing dat hij of zij zich waarschijnlijk niet op een legitieme overheidswebsite bevindt.

HSTS-standaard

De HSTS-standaard is een complementaire standaard die ervoor zorgt dat een internetbrowser eist dat een website altijd HTTPS blijft gebruiken na het eerste contact over HTTPS.[11] Door HTTPS samen met HSTS te gebruiken wordt het gebruik van beveiligde verbindingen zoveel mogelijk afgedwongen. Dit maakt het voor hackers en cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van het webverkeer te onderscheppen of te manipuleren.

4. Inhoud van het voorstel

Dit besluit verplicht bestuursorganen de open standaarden HTTPS en HSTS toe te passen op al hun voor publiek toegankelijke websites en webapplicaties conform de aanbevolen

[9] Hostnames zijn niet versleuteld, tenzij ESNI wordt gebruikt. Het is voor afluisteraars dus nog steeds duidelijk dat iemand bijvoorbeeld overheid.nl bezoekt, maar niet precies welke pagina.
[10] *Spoofing* is ook mogelijk van een gelijkend (maar niet identiek) domein. Bijvoorbeeld: rijks0verheid.nl (met een ‘nul’) in plaats van rijksoverheid.nl. HTTPS sluit die vorm van *spoofing* niet uit en dit dient anders afgevangen te worden.
[11] Dit geldt voor de duur van de door de applicatiebeheerder ingestelde cachingtijd. Bijvoorbeeld een jaar na het laatste bezoek.

configuratie van het NCSC zoals opgenomen in de NCSC-richtlijnen voor TLS-configuratie en webapplicaties. Voor de open standaarden gaat het om de versies IETF RFC 6797 en 2818.[12]

Grondslag

Op grond van artikel 3, tweede lid, van de Wet digitale overheid (WDO) kunnen bij algemene maatregel van bestuur standaarden voor elektronisch verkeer worden aangewezen, die bestuursorganen verplicht dienen toe te passen. Aan de mogelijkheid tot aanwijzing van een standaard stelt de WDO de volgende drie cumulatieve vereisten:

a. De aanwijzing van de standaard is noodzakelijk en proportioneel gelet op de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronische verkeer, dan wel noodzakelijk ter uitvoering van verdragen of bindende besluiten van volkenrechtelijke organisaties.
b. De standaard is tot stand gekomen volgens een voor eenieder toegankelijke procedure.
c. De standaard is openbaar toegankelijk en kosteloos bruikbaar en over de specificaties ervan kan blijvend vrijelijk worden beschikt dan wel blijvend kan worden verkregen tegen een redelijke vergoeding.

De HTTPS- en HSTS-standaard voldoen beide aan deze voorwaarden. Het Forum Standaardisatie heeft deze standaarden in 2017 getoetst en opgenomen op de ‘pas toe of leg uit’-lijst met open standaarden.[13] Bij inwerkingtreding van dit besluit zullen deze open standaarden van de ‘pas toe of leg uit’-lijst worden verwijderd.

Ingevolge artikel 3, derde lid, van de WDO dient in de algemene maatregel van bestuur in ieder geval te worden bepaald: het functionele toepassingsbereik van de aangewezen standaard, de organen waarvoor de verplichting tot toepassing van een aangewezen standaard geldt en de datum waarop de verplichting tot toepassing van een aangewezen standaard ingaat.

Organen

De verplichting tot toepassing van de standaarden geldt voor bestuursorganen 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 rechtspersonen die krachtens publiekrecht zijn ingesteld, en die niet zijn uitgezonderd in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht. Het gaat dan om de organen van de Staat (mits niet uitgezonderd), provincies, gemeenten, waterschappen en andere rechtspersonen die krachtens publiekrecht zijn ingesteld.

[12] Deze standaarden worden beheerd door de *Internet Engineering Task Force* (IETF).
[13] https://www.forumstandaardisatie.nl/standaard/HTTPS-en-HSTS-0. Onderliggende TLS-standaard is vanaf 2014 opgenomen op de lijst: https://www.forumstandaardisatie.nl/standaard/TLS.

De zogenaamde b-bestuursorganen, organen, personen en colleges als bedoeld in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht, alsmede rechtspersonen met een wettelijke taak, voor zover deze geen a-bestuursorgaan zijn, vallen niet onder deze verplichting. Deze bestuursorganen en rechtspersonen vielen ook niet onder het reeds gevoerde beleid. Dit wil overigens niet zeggen dat toepassing van de standaarden op hun websites niet verstandig is.

Functionele toepassingsbereik

De verplichting tot toepassing van de standaarden ziet op alle publiek toegankelijke websites en webapplicaties van a-bestuursorganen. Een website is een samenhangende verzameling van webpagina's met inhoud bestaande uit tekst, foto's en video's. Webapplicaties zijn programma's die draaien op een webserver. Een voorbeeld van een webapplicatie is webmail. Voor websites en webapplicaties is kenmerkend dat deze draaien op een webserver en kunnen worden benaderd via een webbrowser of andere cliënt die HTTP ondersteunt.

Voor het functionele toepassingsbereik van de verplichting is de inhoud en functionaliteit van de website niet relevant. Dit betekent concreet dat de verplichting geldt voor zowel websites (al dan niet na inloggen) waar informatie wordt uitgewisseld met een bezoeker (bijvoorbeeld doormiddel van een applicatie of formulieren) als websites waar (statische) informatie wordt weergegeven. Webapplicaties en Web *application programming interfaces* (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.

Door het verplicht voorschrijven van HTTPS en HSTS voor alle websites zijn bestuursorgaan niet afhankelijk van bijvoorbeeld de inschatting van webbeheerders van wat precies beschouwd moet worden als gevoelige informatie. De mate van gevoeligheid van informatie kan per situatie verschillen. Vergissingen over wanneer HTTPS op zijn plaats is, worden voorkomen door een algeheel voorschrift HTTPS voor alle websites te gebruiken.

Gelet op het doel van de verplichting dient de reikwijdte van de verplichting materieel ingevuld te worden. Het eigendom van de domeinnaam en het beheer van de website zijn daarbij niet relevant. Doorslaggevend is of de website gebruikt wordt in het kader van de uitvoering van een publieke taak door een bestuursorgaan.

De verplichting tot toepassing van de standaarden heeft ook betrekking op ook zogeheten *parking pages* en *redirects*. Een *parking page* is een 'lege' website waarop veelal wordt aangekondigd wie de eigenaar is en welke informatie daar zal verschijnen. Een *redirect* is een domeinnaam die doorverwijst naar een andere website op een andere domeinnaam. Een voorbeeld hiervan is https://www.minbzk.nl dat doorverwijst naar https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties. Toepassing van de standaarden kan achterwege blijven in het geval

dat een domeinnaam wel is geregistreerd, maar er nog geen pagina beschikbaar is gesteld. Aangezien er dan nog geen pagina is om te bezoeken, hoeft die ook niet beveiligd te worden.

Configuratie

Concreet betekent het toepassen van HTTPS dat partijen een TLS-certificaat installeren op hun website. Deze certificaten zijn er in meerdere versies en kunnen met verschillende beveiligingsopties worden toegepast. Dit besluit schrijft geen specifiek type TLS-certificaat voor. Zowel domeinvalidatie-, organisatievalidatie- als uitgebreide validatie-certificaten zijn geschikt om het gewenste beveiligingsniveau te halen. Deze certificaten bieden dezelfde beveiliging maar verschillen in aanvraagproces en in de wijze waarop de gegevens van de eigenaar en certificaatverstrekker worden weergegeven.

Een slechte TLS-configuratie biedt geen goed beveiligde verbinding. De TLS-richtlijnen en de Webapplicaties-richtlijnen van het NCSC geven aan met welke beveiligingsinstellingen de standaarden dienen te worden toegepast voor een veilig resultaat. Daarbij geldt dat dit besluit een minimumeis betreft. Het staat bestuursorganen vrij om strengere beveiligingsinstellingen toe te passen indien zij dit nodig achten.

Dit besluit verwijst naar specifieke versies van de NCSC-richtlijnen. Gekozen is voor een statische verwijzing boven een dynamische verwijzing, om te zorgen dat de inhoud van de verplichting bepaald blijft worden door de regering. Indien het NCSC de richtlijnen wijzigt, dan wijzigt de verplichting op grond van dit besluit niet automatisch mee. In dat geval zal bekeken worden of aanpassing van dit besluit nuttig en noodzakelijk is. Met het NCSC zijn afspraken gemaakt om onder meer te zorgen dat de richtlijnen permanent beschikbaar zijn op de met de verwijzing aangeduide locatie, ook ingeval de richtlijnen door het NCSC worden aangepast. Bestuursorganen die HTTPS en HSTS toepassen, doen er overigens verstandig aan om eventuele wijzigingen in de NCSC-richtlijnen actief te volgen.

Webapplicatie-richtlijn

De ICT-beveiligingsrichtlijnen voor Webapplicaties van het NCSC zijn gericht op websites waarmee gevoelige of vertrouwelijke informatie wordt uitgewisseld, bijvoorbeeld door middel van contactformulieren en entreepagina's die daarbij horen. Dit besluit gaat verder en verplicht het toepassen van deze beveiligingsrichtlijnen voor *alle* via internet toegankelijke websites van bestuursorganen ongeacht de inhoud of functionaliteit van de website. Dit sluit aan bij de reikwijdte van de streefbeeldafspraak van het OBDO met betrekking tot het toepassen van deze standaarden.

TLS-richtlijn

Het NCSC maakt in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) onderscheid tussen vier configuratieniveaus: 'goed', 'voldoende', 'uit te faseren' en 'onvoldoende'. Het NCSC stelt dat van 'uit te faseren'**-**instellingen bekend is dat deze fragiel zijn met het oog op de doorontwikkeling van aanvalstechnieken. Dit houdt in dat het risico bestaat dat deze instellingen in de nabije toekomst de status 'onvoldoende' krijgen.

Om die reden adviseert het NCSC organisaties 'uit te faseren'**-**configuraties te verwijderen zodra de mogelijkheid zich daartoe aandient en hier niet afwachtend mee om te gaan. Een voorbeeld van een uit te faseren instelling is het gebruik van de verouderde TLS-versies 1.0 en 1.1. Een reden om deze nog niet uit te faseren is bijvoorbeeld dat websites voorzien van de verouderde TLS-versies bezocht kunnen worden door gebruikers met (zwaar) verouderde besturingssystemen en browsers, waar de softwarevereisten van de meer recente (en veiliger) TLS-versies ook meer recente besturingssystemen en browsers vereisen om te functioneren.

Het NCSC noemt mede daarom geen deadline voor de uit te faseren instellingen en laat dit aan individuele organisaties. Een aantal recente ontwikkelen maakt dat dit besluit wel een dergelijke deadline geeft (zie onder paragraaf 8). Na inwerkingtreding van dit besluit dient TLS geconfigureerd te zijn op ten minste niveau 'voldoende'.

Deze ontwikkelingen zijn:

1. De makers van de meest gebruikte browsers: Chrome (Google), Firefox (Mozilla), Safari (Apple) en IE/EGDE (Microsoft) hebben aangekondigd de ondersteuning van TLS-versie 1.0 en 1.1 te stoppen in de eerste helft van 2020.[14] Dit betekent concreet dat overheidswebsites die niet ten minste zijn voorzien van TLS-versie 1.2 (NCSC-niveau 'voldoende') in de tweede helft van 2020 niet meer via die browsers bezocht kunnen worden.
2. De ondersteuning voor de tweede generatie PKIoverheid-certificaten, die door veel overheidsorganisaties gebruikt worden,[15] stopt per 25 maart 2020. De softwarevereisten voor de derde generatie PKIoverheid-certifcaten of PKIo *Extended Validation*-certificaten, waar deze organisaties op overgaan, zijn gemiddeld strikter dan de softwarevereisten voor TLS-versie 1.2.[16] Waar veel organisaties momenteel nog oudere TLS-versies ondersteunen om websitebezoekers met (zwaar) verouderde software tegemoet te komen, kan dit dadelijk door deze maatregel niet meer. Logius is een voorbeeld van een

[14] https://www.computerworld.com/article/3313589/big-browsers-to-pull-support-plug-for-tls-10-and-11-encryption-protocols-in-early-20.html.
[15] In de steekproef van Innovalor gebruikt bijna 40% van de overheidsdomeinen een PKIo certificaat: https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/documenten/rapporten/2019/03/13/pki-overheid---onderzoek-naar-mogelijkheden-om-gebruik-te-vergroten-bijvoorbeeld-via-verplichtstelling.
[16] Alleen bij het gebruik van Windows ligt het minimum iets hoger, namelijk ten minste Windows 7 in plaats van Vista. Zie: http://crl.pkioverheid.nl/pkiotest/ en https://www.projectdatasphere.org/projectdatasphere/html/tls/faq.

organisatie die met het oog op de certificaatvervanging, tegelijk de ondersteuning van TLS 1.0 en 1.1 op de publieke DigiD-domeinen heeft stopgezet.

3. De verwachte impact van de deadline is beperkt. Wereldwijd is het aantal websites dat TLS-versie 1.2 ondersteunt reeds hoog. Uit wekelijkse testen van Mozilla blijkt bovendien dat er van de één miljoen geteste populaire websites wereldwijd die TLS toepassen, in nog maar 0,6% van de gevallen alleen TLS-versies 1.0 en 1.1 worden toegepast. De overige websites bieden daarnaast allemaal ten minste TLS-versie 1.2 aan.[17] Exacte cijfers van websites van bestuursorganen zijn niet bekend, maar de impact van het uitfaseren van TLS-versies 1.0 en 1.1 is hier naar verwachting eveneens beperkt. Mede om die reden hebben veel organisaties reeds TLS-versies 1.0 en 1.1 uitgefaseerd of zijn daar nu mee bezig. Een paar voorbeelden zijn: www.digid.nl, www.s-hertogenbosch.nl, www.promovendum.nl en www.snsbank.nl. Deze sites gebruiken alleen nog TLS-versie 1.2 (en hoger).

Gebruikers met software die al jaren niet meer geüpdatet wordt, kunnen door de genoemde ontwikkelingen en inwerkingtreding van dit besluit geen overheidswebsite meer bezoeken. Zoals gezegd is deze groep naar verwachting erg klein en wordt bovendien steeds kleiner.

Dienst Publiek en Communicatie van het ministerie van Algemene Zaken houdt de bezoekersstatistieken bij van ruim 500 overheidswebsites. Daaruit blijkt dat bij 0,3 % van de bezoeken in 2019, besturingssystemen en browsers gebruikt werden, die niet in staat zijn TLS 1.2 te ondersteunen. Deze besturingssystemen zijn dermate verouderd dat hier geen moderne browsers voor beschikbaar zijn.

In alle andere gevallen wordt TLS 1.2 reeds door de software van de bezoekers ondersteund, of is eenvoudig en kosteloos de gebruikte browser te updaten naar een versie die TLS 1.2 wel ondersteund.

Bovendien lopen bezoekers met verouderde software zelf een steeds groter beveiligingsrisico door met de verouderde software internet te gebruiken. Door deze groep tegemoet te blijven komen met verouderde beveiligingsopties op overheidswebsites, houdt de overheid een ongewenste situatie in stand. De overheid geeft hen door dit besluit een belangrijk signaal, dat het van belang is om actuele en geüpdatete software te gebruiken.

5. Verhouding tot andere regelgeving en beleid

Regelgeving

Ingevolge artikel 32, eerste lid, van de Algemene verordening gegevensbescherming dienen passende technische en organisatorische maatregelen te worden getroffen om persoonsgegevens te beveiligen. De maatregel kan omvatten de versleuteling van persoonsgegevens. Voor zover via een website persoonsgegevens worden uitgewisseld

[17] https://hacks.mozilla.org/2019/05/tls-1-0-and-1-1-removal-update.

(bijvoorbeeld door middel van formulieren) is de Autoriteit persoonsgegevens van oordeel dat organisaties verplicht zijn HTTPS toe te passen.[18] Dit besluit geeft concrete invulling aan deze algemene beveiligingsverplichting en gaat verder dan waartoe de verordening verplicht, nu de beveiligingsplicht uit hoofde van dit besluit zal gelden voor ieder type informatie dat via de website uitgewisseld wordt.

Beleid

In een aantal gevallen wordt het gebruik van HTTPS en HSTS reeds voorgeschreven. Zo dienen bestuursorganen die gebruik maken van DigiD, volgens de Norm ICT-beveiligingsassessments DigiD gebruik te maken van HTTPS en HSTS.[19] Ook in de Baseline Informatiebeveiliging Overheid (hierna: BIO) wordt het gebruik van HTTPS en HSTS voorgeschreven. In de BIO staat onder 13.2.3.1.: “Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de ‘pas toe of leg uit’-lijst van het Forum.” In beide gevallen sluit dit aan bij de reikwijdte van dit besluit.

6. Gevolgen

Overheden

Dit besluit brengt voor a-bestuursorganen de verplichting mee de open standaarden HTTPS en HSTS te hanteren voor publiek toegankelijke websites. Voor wat betreft de financiële gevolgen van deze verplichting is relevant dat deze open standaarden momenteel al door de bestuursorganen (moeten) worden gehanteerd. Dit betekent dat de bestuursorganen die de betreffende open standaarden reeds hebben geïmplementeerd geen financiële gevolgen ondervinden van het verplicht stellen van de standaarden. Voor het geval het orgaan de standaarden nog niet hanteren, zijn de implementatiekosten hiervan per website ingeschat.

In 2015 heeft het Forum Standaardisatie voor het Nationaal Beraad Digitale Overheid een inschatting gemaakt van de kosten van het implementeren van HTTPS op een gemiddelde website.[20] Kort gezegd kan dit in het meest gunstige geval zonder kosten, of afhankelijk van de situatie en keuzes van de bestuursorganen zelf, voor een bedrag van een paar honderd euro per website per twee à drie jaar.

Een aantal leveranciers van domeinen en websites past HTTPS en HSTS toe zonder extra kosten. De Dienst Publiek en Communicatie van het ministerie van Algemene Zaken zorgt er bijvoorbeeld voor dat HTTPS voor alle websites op het Platform Rijksoverheid Online beschikbaar is en veilig is geconfigureerd en brengt daarvoor geen aanvullende kosten in rekening.

Een aantal bestuursorganen maakt gebruik van een eigen webserver. In dat geval zijn, naar inschatting van Forum Standaardisatie, de eenmalige kosten voor het configureren

[18] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht?qa=https&scrollto=1.
[19] Zie https://www.logius.nl/diensten/digid/ict-beveiligingsassessments.
[20] https://digitaleoverheid.pleio.nl/file/download/41528772.

van HTTPS en HSTS op de webserver maximaal € 400, en jaarlijkse kosten voor het beheren en aanpassen van HTTPS- en HSTS-configuratie op de webserver en voor het beheer van het sleutelmateriaal eveneens maximaal € 400.

Er zijn, zoals gezegd, drie soorten TLS-certificaten: domeinvalidatie, organisatievalidatie en uitgebreide validatie. Deze certificaten bieden dezelfde beveiliging maar verschillen in aanvraagproces en in de wijze waarop de gegevens van de eigenaar en certificaatverstrekker worden weergegeven. In die situaties dat er nog geen verplichting of beleid bestaat om een specifiek type certificaat toe te passen, is het aan bestuursorganen zelf welk type certificaat zij willen toepassen. Hierdoor zijn de potentiële kosten vanaf € 0,- (in geval van een gratis domeinvalidatie-certificaat) tot € 600,- voor drie jaar, bij de aanschaf van een PKIoverheid-certificaat.

Burgers en Bedrijven

De verplichting om HTTPS en HSTS toe te passen op overheidswebsites heeft geen financiële gevolgen voor burgers en bedrijven. Alle gangbare courante versies van de internetbrowsers, zoals Chome, Safari, Firefox en Internet Explorer, ondersteunen de standaarden reeds. Burgers en bedrijven hoeven niets te doen om van het voordeel van een veilige, privacy beschermende verbinding met een overheidswebsite te kunnen profiteren.

7. Uitvoering, toezicht en handhaving

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.[21] 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.

[21] https://www.forumstandaardisatie.nl/thema/monitor-open-standaarden.

8. Overgangsrecht en inwerkingtreding

Dit besluit treedt in werking op [datum] en heeft onmiddellijke werking. Nu bestuursorganen zichzelf eerder hebben verbonden aan de streefbeeldafspraak om vóór 2019 te voldoen aan de standaarden, en gelet op de ontwikkelingen genoemd in paragraaf 4, is er geen noodzaak voor overgangsrecht.

9. Advies en consultatie

Internetconsultatie

PM

Autoriteit persoonsgegevens

PM

Adviescollege toetsing regeldruk

PM

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,