Besluit van
houdende aanwijzing van de open informatieveiligheidsstandaarden HTTPS en HSTS voor overheidswebsites (Besluit veilige overheidswebsites)

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. *NCSC*-richtlijnen: de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) gepubliceerd op https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.

Artikel 2. Aanwijzing

De organen, genoemd in artikel 3, eerste lid, van de Wet digitale overheid, beveiligen hun websites, voor zover die publiek toegankelijk zijn, door toepassing van de standaarden HTTPS en HSTS, overeenkomstig de instellingen genoemd in hoofdstuk 4 van de NCSC-richtlijnen.

Met opmerkingen [HF1]: Open norm. Bij voorkeur verwijzen naar een register van dergelijke sites oid.

Artikel 3. Inwerkingtreding

Dit besluit treedt in werking met ingang van 1 januari 2020.

Artikel 4. Citeertitel

Dit besluit wordt aangehaald als: Besluit veilige overheidswebsites.

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 websites van overheidsorganen gericht op dienstverlening aan bezoekers zoals burgers, bedrijven en andere overheden. Het besluit heeft tot doel de beveiliging van overheidswebsites te bevorderen. Bezoekers van overheidswebsites moeten erop kunnen vertrouwen dat de informatie die zij op die website verkrijgen op een veilige manier verloopt daadwerkelijk van die overheidspartij afkomstig is en dat tegelijk de privacy van de bezoeker geborgd wordt, doordat de verbinding met de website beveiligd is.

Met opmerkingen [HF2]: Dat wordt niet door deze standaarden geregeld.

2. Aanleiding

In februari 2017 is aan de Tweede Kamer de toezegging gedaan om de toepassing van de HTTPS-standaard bij overheidswebsites te verplichten.[1] 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 overheidsorgaan 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). Overheidsorganen hebben de mogelijkheid af te wijken van de voorgeschreven 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.[2]

Begin 2018 is het Nationaal Beraad opgevolgd door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Het OBDO besloot begin 2018 het streefbeeld van het Nationaal Beraad te verlengen en uit te breiden, opdat alle overheidswebsites HTTPS en HSTS toepassen voor het einde van 2018 en deze conform de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) configureren.[3]

Met opmerkingen [PK3]: Verwijzing instellingsbesluit OBDO toeveogen? https://zoek.officielebekendmakingen.nl/stcrt-2018-9728.html

Met opmerkingen [VMVd4]: De link verwijst naar de 2014 versie van het whitepaper. Zodra de 2019 gepubliceerd wordt (naar verwachting in maart 2019) wordt die versie in deze AMvB aangehouden voor een veilige configuratie.

[1] *Kamerstukken II* 2016/17, 26643, nr. 443, p. 11-12 en *Kamerstukken II* 2018/19, 26643, nr. 574, p. 5-6.
[2] https://digitaleoverheid.pleio.nl/file/download/44041112.
[3] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

De meest recente open standaarden-meting van het Forum Standaardisatie laat zien dat dit streefbeeld van 100% waarschijnlijk niet gehaald wordt. In september 2018 was het aantal overheidswebsites dat HTTPS toepaste weliswaar 96%, maar toepassing op de door het NCSC geadviseerde veilige wijze slechts 64%. Nu het huidige beleid niet tot gevolg heeft dat alle overheidsorganen de standaarden hebben geïmplementeerd, worden deze 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. Het is daarom belangrijk dat overheidsorganen hun websites goed beveiligen.

Gebruikers en overheidsorganen dienen veilig met elkaar te kunnen communiceren en moeten bij het bezoeken van overheidswebsites erop kunnen vertrouwen dat hun veiligheid en privacy, alsmede de veiligheid en betrouwbaarheid van de keten, geborgd is. Het verplichtstellen van de HTTPS- en HSTS-standaarden is om die reden proportioneel nu het huidige beleid niet tot gevolg heeft dat alle overheidspartijen de standaarden hebben geïmplementeerd. Daar komt bij dat de maatschappelijke baten van het toepassen van de standaarden voor bezoekers van websites groter zijn de dan de uitvoeringslasten van individuele overheidsorganen.

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.

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. 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.

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.

Met opmerkingen [HF5]: Gaat het dan om publieke websites? Anders richt de AMvB zich op iets anders dan het onderzoek.

Met opmerkingen [VMVd6]: Eind maart 2019 doet Forum Standaardisatie een nieuwe meting. De resultaten worden hier ingevoegd.

De verwachting (op basis van een snelle steekproef) is dat zowel HTTPS en HSTS beiden nog niet 100% worden toegepast.

Met opmerkingen [PK7]: Is het nog waardevol een zin te wijden aan wanneer het nCSC-niveau gevolgd moet worden.
Wordt dat in de meting van het Forum ook telkens inzichtelijk gemaakt en is aanscherrping van de doelstelling van OBDO (naar niveau NCSC) nog waardevol?

Met opmerkingen [PK8]: Zou misschien ook goed zijn om aan te geven dat de overheid steeds meer zaken digitaal voorschrijft. OF dat burgers en bedrijven steeds meer verlangen dat overheid digitaal bereikbaar is.

Met opmerkingen [HF9]: Dat wordt toch niet met die standaarden geregeld?

Met opmerkingen [HF10]: Als ik het goed begrijp, valt dat wel mee, maar hebben ze het niet op de juiste manier gedaan.

Met opmerkingen [HF11]: Je voorkomt toch niet *.1eiden.nl?

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. 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.[4]

De toepassing van HTTPS is inmiddels gemeengoed.

De Nederlandse overheid loopt met deze maatregel niet op de troepen vooruit. Het wordt buiten de overheid steeds moeilijker nog websites te vinden die niet voorzien zijn van HTTPS. ~~Als eerst~~Ten eerste doordat er steeds meer websites gebruik maken van HTTPS, daarnaast wordt letterlijk het 'vinden' van deze websites lastiger, omdat populaire zoekmachines, zoals Google, websites zonder HTTPS lager in de zoekresultaten plaatsen. Google duidt in de eigen browser: Chrome, websites zonder ~~https~~ HTTPS sinds juli 2018 bovendien aan als "onveilig".[5] Echter dat is nog niet voldoende, omdat gebruikers vaak ongemerkt naar een onbeveiligde website worden geleid (of iets dergelijks…anders klinkt het misschien alsof we niets hoeven te doen?)

Ook andere overheden zetten in op de toepassing van HTTPS. Het CIO office van de Amerikaanse overheid hanteert 'HTTPS for everything' als norm[6]. 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.

Met opmerkingen [HF12]: Ik heb dit gevoel ook, maar vind het lastig zonder feitelijke onderbouwing.

Met opmerkingen [PK13]: Benadrukken van grenzeloosheid internet ook nog relevant?

Met opmerkingen [HF14]: Weglaten, want los je niet op met deze standaarden.

Met opmerkingen [HF15]: Wat voor norm? Is dat equivalent aan de PTOLU norm?

Met opmerkingen [PK16]: Misschien kan je deze alinea na de eerste zin plaatsen.

4. Inhoud van het voorstel

Dit besluit verplicht overheidsorganen de HTTPS- en HSTS-standaard toe te passen op al hun voor publiek toegankelijke websites conform de aanbevolen configuratie op niveau "goed" van het NCSC zoals opgenomen in de ICT-beveiligingsrichtlijnen voor Transport Layer Security. Voor de open standaarden gaat het om de versies IETF RFC 6797 en 2818.[7] De configuratie staat beschreven in 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' uit 2014[8].

Met opmerkingen [HF17]: Dit vereist aandacht.

Met opmerkingen [VMVd18]: Let op: Deze AMvB zal de richtlijnen gaan hanteren uit 2019. Deze worden naar verwachting komende maand gepubliceerd.
Op het moment dat deze verschijnen, wordt de tekst en verwijzing daarop aangepast.

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 overheidsorganen verplicht dienen toe te passen. Aan de mogelijkheid tot aanwijzing van een standaard stelt de WDO de volgende drie cumulatieve vereisten:

- De aanwijzing van de standaard is noodzakelijk en proportioneel gelet op de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid

[4] De toepassing van HSTS naast HTTPS is een aanbeveling van het NCSC: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html.
[5] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html
[6] https://https.cio.gov/everything/
[7] Deze standaarden worden beheerd door de *Internet Engineering Task Force* (IETF).
[8] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

of de doelmatigheid van het elektronische verkeer, dan wel noodzakelijk ter uitvoering van verdragen of bindende besluiten van volkenrechtelijke organisaties.
- De standaard is tot stand gekomen volgens een voor eenieder toegankelijke procedure.
- 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-standaarden voldoen aan deze voorwaarden. Het Forum Standaardisatie heeft de standaarden in 2017 getoetst en opgenomen op de zogenaamde 'pas toe of leg uit'-lijst met open standaarden.[9] 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.

Toepassingsbereik

De verplichting tot toepassing van de standaarden geldt voor alle organen genoemd in artikel 3, eerste lid, van de WDO. Het gaat hier om bestuursorganen, organen, personen en colleges als bedoeld in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht en rechtspersonen met een wettelijke taak als bedoeld in artikel 1.1 van de Comptabiliteitswet 2016.

De verplichting omvat alle publiek toegankelijke websites van overheidsorganen ongeacht de inhoud of functionaliteit van de website. Dit betekent concreet dat de verplichting geldt voor zowel websites waar informatie wordt uitgewisseld met een bezoeker (bijvoorbeeld door middel van formulieren) als websites waar (statische) informatie wordt weergegeven.

Door het verplichten van HTTPS voor alle websites ben je als overheid niet afhankelijk van ~~de soms subjectieve inschatting~~ van bijvoorbeeld de inschatting van webbeheerders van wat precies beschouwd moet worden als gevoelige informatie. Vergissingen over wanneer HTTPS op zijn plaats is, worden voorkomen door een algeheel voorschrift HTTPS voor alle websites te gebruiken.

Dit de verplichting omvat ook zogeheten *parking pages* en *redirect pages*. Een *parking page* is een 'lege' website waarop veelal wordt aangekondigd wie de eigenaar is en welke informatie daar zal verschijnen. Een *redirect page* is website die doorverwijst naar een andere website. Een voorbeeld hiervan is https://www.minbzk.nl die doorverwijst https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties. Ook deze websites bevatten informatie respectievelijk

Met opmerkingen [HF19]: Werkt dit ook door op in de markt uitbestede websites?

Hoe werkt dit door op websites van publiek private samenwerkingen?

Met opmerkingen [HF20]: Dus geen intranet sites.

Met opmerkingen [HF21]: Dat klopt, maar een oordeel over noodzaak van de beveiliging van gevoelige informatie, moet sowieso ook een zaak zijn van andere partijen, zoals CISO.

[9] 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.

doorverwijzingen waarbij de bezoeker ervan uit moet kunnen gaan dat die van een legitieme partij zijn. Wanneer deze paginaś niet beveiligd zijn ontstaan er ongewenste veriligheidrisicoś etc.

Toepassing van de standaarden kan achterwege blijven in het geval dat een domeinnaam wel alvast is geregistreerd, maar ~~waar~~ er nog geen ~~website~~ pagina beschikbaar is gesteld. Aangezien er dan nog geen pagina is om te bezoeken, hoeft die ook niet beveiligd te worden. De standaarden behoeven evenmin te worden toegepast op websites die niet publiek toegankelijk zijn. Voorbeelden hiervan zijn intranetten en besloten samenwerkingsruimten.

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 overheidsorgaan.

Met opmerkingen [HF22]: Hoe?

Met opmerkingen [HF23]: Doelt dit op uitbesteding?

Met opmerkingen [HF24]: Het gaat toch om publieke toegankelijkheid?

Met opmerkingen [PK25]: Mooi!

Configuratie

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

Een slechte configuratie biedt alsnog geen goed beveiligde verbinding. De ICT-beveiligingsrichtlijnen voor TLS van het NCSC geven aan welke TLS-versies veilig beschouwd worden en met welke beveiligingsinstellingen deze het best kunnen worden toegepast voor een optimaal veilig resultaat. Dit besluit sluit aan op de richtlijn die voorschrijft dat de instellingen ten minste moeten voldoen aan het niveau 'voldoende', zoals omschreven in hoofdstuk 4 van de richtlijn[10]. Het betreft hier een minimumeis. Het staat overheidsorganen vrij om strengere beveiligingsinstellingen toe te passen.

5. Verhouding tot andere regelgeving en beleid

Er zijn reeds wettelijke verplichtingen en beleidskaders die toepassing van HTTPS in bepaalde gevallen voorschrijven. Meer specifiek gaat het hier om de Algemene verordening gegevensbescherming en de Baseline Informatiebeveiliging Overheid.

[10] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

De Algemene verordening gegevensbescherming

Ingevolge artikel 32, eerste lid, van de Algemene verordening gegevensbescherming dienen passende technische en organisatorische maatregelen te worden getroffen om persoonsgegevens te beveiligen. Deze maatregel kan omvatten de versleuteling van persoonsgegevens. Voor zover via een website persoonsgegevens worden uitgewisseld (bijvoorbeeld door middel van formulieren) is de Autoriteit persoonsgegevens van oordeel dat organisaties verplicht zijn HTTPS toe te passen.[11]

Dit besluit geeft concrete invulling aan deze algemene beveiligingsverplichting. Voorliggende besluit gaat overigens verder dan waartoe de AVG verplicht, nu de beveiligingsplicht uit hoofde van dit besluit zal gelden voor ieder type informatie.

De Baseline Informatiebeveiliging Overheid

De Baseline Informatiebeveiliging Overheid (BIO) [12]bevat een groot aantal minimumeisen voor informatieveiligheid waaraan organen van het Rijk, gemeenten, provincies en waterschappen moet voldoen. De BIO omvat één gezamenlijk normenkader voor informatieveiligheid waaraan een orgaan in ieder geval moet voldoen om vertrouwelijkheid, ~~juistheid~~ integriteit en beschikbaarheid van gegevens en systemen te organiseren. Sinds 1 januari 2019 vindt de implementatie van de BIO bij alle bestuurslagen van de overheid plaats. Gestreefd wordt om vanaf 1 januari 2020 volgens de BIO te werken en verantwoorden.

Op grond van de BIO dienen overheidsorganen bij voorkeur gebruik~~t~~ te maken van PKIoverheid-certificaten bij webverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de Rijksdienst waar gebruikers rechten aan kunnen ontlenen.[13]

Ook hier gaat de verplichting uit hoofde van voorliggende besluit verder dan waartoe de BIO verplicht. Bij uitwisseling van ieder type informatie via een overheidswebsite moet de bezoeker erop kunnen vertrouwen dat dit veilig en vertrouwelijk verloopt. Niet alleen bij de uitwisseling van informatie waar de bezoeker rechten aan kan ontlenen. Met als belangrijke verschil dat het voorliggende besluit daarbij geen voorwaarden stelt aan het type certificaat dat wordt toegepast.

6. Gevolgen

Overheden

Dit besluit brengt voor overheidsorganen de verplichting mee de open standaarden HTTPS en HSTS te hanteren voor websites. Voor wat betreft de financiële gevolgen van deze

Met opmerkingen [VMVd26]: Kan nog niet verwijzen naar de BIO, want deze is nog niet gepubliceerd?

Met opmerkingen [HF27R26]: Gaat snel gebeuren.

Met opmerkingen [HF28]: Voor de BIR geldt i.i.g. dat implementatie alleen geldt voor nieuwe systemen en bij actualisatie van systemen. In andere gevallen is BIR 2012 nog steeds van kracht.

Met opmerkingen [KS29]: Dit is geen verplichting.

Met opmerkingen [HF30]: Publiek toegankelijk?

[11] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht?qa=https&scrollto=1.

[12]

[13] Een PKIoverheid-certificaat is een TLS-certificaat dat onder bepaalde voorwaarden en met een specifiek procedure wordt uitgegeven. Dit geeft extra zekerheid over de herkomst van het certificaat.

verplichting is relevant dat deze open standaarden al door de overheidsorganisaties (moeten) worden gehanteerd. Dit betekent dat de overheidsorganen die de betreffende open standaarden reeds hebben geïmplementeerd geen financiële gevolgen ondervinden van het verplicht stellen van een standaard. Voor het geval de overheidsorganisaties de standaarden nog niet hanteerden, 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[14]. Kort gezegd kan dit in het meest gunstige geval zonder kosten, of afhankelijk van de situatie en keuzes van de organisaties zelf, voor een bedrag van een paar honderd euro per website per aantal jaren.

Een aantal leveranciers van domeinen en/of 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.

heeft opmaak toegepast: Standaardalinea-lettertype

Een aantal overheidsorganen maakt gebruik van hun eigen webserver die nog niet aan de eisen voldoet. Het orgaan maakt dan, naar inschatting van het Bureau Forum Standaardisatie, eenmalige kosten voor het configureren van TLS en HSTS op webserver van maximaal € 400 en jaarlijkse kosten voor het beheren en aanpassen van TLS- en HSTS-configuratie op de webserver en voor het beheer van het sleutelmateriaal eveneens maximaal € 400.

Aanschaf TLS-certificaat

Er zijn, zoals gezegd, drie soorten TLS-certificaten: domeinvalidatie, organisatievalidatie en uitgebreide validatie. Deze certificaten bieden dezelfde beveiliging maar verschillen 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 overheidsorganisaties 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 internbrowsers, zoals

[14] https://digitaleoverheid.pleio.nl/file/download/41528772

bijvoorbeeld Internet Explorer, Safari, Firefox en Chrome, ondersteunen de standaarden reeds. Burgers en bedrijvenf hoeven niets te doen om van het voordeel, een veilige, privacy beschermende verbinding met een overheidswebsite te kunnen profiteren.

7. Uitvoering, toezicht en handhaving

Het Bureau Forum Standaardisatie meet jaarlijks in hoeverre de standaarden op de 'pas toe of leg uit'-lijst worden toegepast. Door de Minister aangewezen open standaarden worden hierin meegenomen.[15] De uitkomsten van de meting worden besproken in het Forum Standaardisatie en worden vervolgens aan het Overheidsbreed Beleidsoverleg Digitale Overheden en vervolgens aan de Tweede~~de 2~~e Kk~~amer~~ voorgelegd.

Het toezicht op de naleving vindt verder plaats overeenkomst het bepaalde in hoofdstuk 6 van de WDO. Onze Minister die het aangaat houdt toezicht op overheidsorganen op het niveau van het Rijk. Voor het overige geldt het reguliere interbestuurlijk toezicht.

Met opmerkingen [KS31]: Hier moeten we nog even goed kijken naar verhouding toezicht vanuit diverse regimes in WDO. Deze regeling regelt dus geen toezicht, maar monitoring door BFS. Wat als een orgaan zich niet aan https houdt? Wat doen we dan?

8. Overgangsrecht en inwerkingtreding

Dit besluit treedt in werking op 1 januari 2020 en heeft onmiddellijke werking. Nu overheidsorganen zichzelf reeds verbonden hebben aan het streefbeeld om vóór 2019 te voldoen aan de standaarden, 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,

drs. R.W. Knops

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