Vraag 1 van 3
Wilt u reageren op Besluit beveiligde verbinding met overheidswebsites en -webapplicaties? Dan kunt u hier uw reactie geven. U kunt dat doen door een bericht achter te laten of door een document te downloaden.

Over het algemeen ben ik goed te spreken over het Besluit beveiligde verbinding met overheidswebsites en -webapplicaties. Ik zie dat er op veel details wordt ingegaan en dat daar goede keuzes gemaakt zijn (bv. om ook redirects en geparkeerde domeinen tot HTTPS/HSTS te verplichten). Ik heb echter nog een paar opmerkingen/aanbevelingen.

Mijn grootste kritiek is op de specifieke verwijzing naar de NCSC-richtlijnen, vooral de TLS-richtlijn. Ik begrijp dat de regering graag de inhoud van dit Besluit bepaald, maar in het huidige Besluit wordt er ook al een groot beroep gedaan op de NCSC-richtlijnen. Waarom kan er niet gewoon vertrouwd worden dat zij in nieuwe versies van hun richtlijnen goede wijzigingen doorvoeren? Heeft de regering voor de huidige versies van de richtlijnen zich al actief gemengd in het opstellen daarvan dan? Mijn probleem met het statisch verwijzen naar de richtlijnen is dat deze zeer snel kunnen en zullen veranderen. Van de een op de andere dag kan een algoritme of hashfunctie gekraakt worden en daarmee in één keer onveilig zijn. Hoe snel gaat de regering dan dit Besluit wijzigen? Sinds de toezegging van de minister in 2017(!) heeft het ook een kleine 3 jaar geduurd voordat dit Besluit er lag/ingevoerd wordt. Als er een belangrijke wijziging door het NCSC doorgevoerd wordt als reactie op onveilige geworden technieken dan moet je het liefst binnen een dag je software bijwerken/instellingen aanpassen. Als de verwachting is dat dit Besluit binnen een maand na zo'n wijziging van de situatie (hetzij nadat het algemeen bekend is geraakt, hetzij na wijziging van de NCSC-richtlijnen) door de regering aangepast wordt dan lijkt me dat nog oké. Als dit langer dan een maand duurt dan is het mijns inziens niet acceptabel omdat de verplichte minimale beveiliging van de verbindingen dan te lang te zwak is. Ik vermoed dat dit laatste het geval is en raad daarom ten strengste aan om dynamisch te verwijzen naar (de laatste versies van) de NCSC-richtlijnen.

Ik lees in de TLS-richtlijn dat in het geval van een acute wijziging deze doorgevoerd wordt aan de huidige versie van de richtlijn. Hopelijk vangt dit mijn hierboven genoemde kritiek af en betekent dit dus zo'n wijziging van de TLS-richtlijn geldig is voor dit Besluit. Wellicht is het een goed idee om hier explicieter over te zijn in het Besluit.

Een gerelateerde vraag. Hoe vaak verwacht de NCSC nieuwe versies van de NCSC-richtlijnen uit te brengen? En hoe lang verwacht de regering er dan over te doen om een nieuw Besluit te maken waarin deze worden opgenomen? Kan hier een maximale termijn aan verbonden worden?

Verder mis ik nog informatie over bepaalde technieken/instellingen:
- Ik lees niks over 'HSTS preload', dit lijkt mij zinnig om op te nemen als best practise
- De 'HSTS max-age'-instelling wordt volgens mij nergens genoemd. Ik zou aanbevelen om deze op minimaal 1 jaar te zetten.
- Ik mis informatie over CAA (DNS Certification Authority Authorization), dit instellen zou ook een best practice moeten zijn

- DNSSEC wordt nauwelijks genoemd, ik zou dit ook verplichten aangezien het een belangrijk onderdeel is van het opzetten van een volledig beveiligde verbinding
- Volgens mij staat er nergens iets over het configureren van HTTP naar HTTPS redirects. Met HSTS lijkt dit overbodig, maar het is goed om ook deze configuratie goed in te stellen. De reactie van 'secubeter.nl (E.M. van Straten)' raakt hier aan en gaat verder ook goed in veel voorkomende verkeerde configuraties. Het is een goed idee om deze dingen expliciet te noemen (in de NCSC-richtlijnen)
- De scans van internet.nl kijkt ook of een website de juiste security options heeft geconfigureerd, in de Webapplicatie-richtlijn wordt een deel daarvan genoemd, maar niet allen. Het lijkt me goed om informatie over alle security options die internet.nl noemt op te nemen: https://internet.nl/faqs/appsecpriv/
- Ik mis informatie over wildcard certificates. Gebruik hiervan kan het configureren van (nieuwe) websites vergemakkelijken en het zorgt ervoor dat websites die (nog) niet publiekelijk gedeeld zijn niet te vinden zijn in Certificate Transparency logs
- Volgens mij valt beveiliging van verbinding voor e-mail niet onder dit Besluit. Dat zou een gemiste kans zijn aangezien deze vaak nog onveiliger geconfigureerd zijn dan websites en wat mij betreft ook vallen onder 'beveiligde verbinding met overheidswebsites en -webapplicaties' (met de nadruk op webapplicaties).

PS: het belang van dit Besluit is groot. Dat wordt onderstreept door het feit dat internetconsultatie.nl zelf nog niet aan de gestelde eisen voldoet (het certificaat is enkel geldig voor 'www.internetconsultatie.nl' en niet voor 'internetconsultatie.nl' wat resulteert in de slecht 'T'-score op SSL Labs; en er wordt geen gebruik van HSTS gemaakt), waardoor ik niet met 100% zekerheid kan stellen dat de informatie die ik over deze consultatie via deze verbinding heb opgehaald niet gemanipuleerd is :D. Fijn dat dit na de invoering van het Besluit beter geregeld moet zijn!

Vraag 2 van 3

Wat vindt u van het toepassingsbereik van de verplichting om de beveiligingsstandaarden toe te passen? Moeten meer of minder organisaties onder deze wettelijke verplichting vallen?

Te veel (overheids)organisaties denken nog dat het maken van een nieuwe website/de aanschaf van een nieuwe server een eenmalige onderneming is die eens in de 5-10 jaar gedaan moet worden. Internetstandaarden en best practices ontwikkelen zich echter continu en in hoog tempo. De beveiligingsstandaarden zijn daarvan de meest basale en belangrijke en horen door zo veel mogelijk organisaties gemonitord en toegepast te worden. ICT wordt steeds belangrijker dus verplichting hiervan lijkt mij goed.

Vraag 3 van 3

De beveiligingsstandaarden moeten ingesteld worden conform de richtlijnen van het Nationaal Cyber Security Centrum. Wat vindt u van het idee om te bepalen dat de

instellingen die in de richtlijn de kwalificaties 'uit te faseren' krijgen, op termijn (bv. 1 juli 2020) verwijderd moeten worden?

Ik vind het goed dat deze verwijderd worden. Hopelijk kan dit dus met een addendum van de richtlijnen en zijn deze dan meteen geldig volgens dit Besluit en hoeft er niet gewacht te worden op een nieuw Besluit. Dit soort aanpassingen zijn dynamisch en wil je ook dynamisch weer kunnen wijzigen. Zoals ik aangaf in mijn reactie op vraag 1 is dat erg belangrijk en vind ik het huidige Besluit daarop tekort schieten.